FortiManager - New Features Guide

Version 6.4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 15, 2022
FortiManager 6.4.0 New Features Guide
02-640-617435-20221115

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-07-05	Added Support for cloud-init service for KVM, Azure, and AWS 6.4.1 on page 30.
2022-04-20	Updated Interface-based shaping profiles and monitoring on page 73.
2021-10-08	Added Normalized interface to map as zone only 6.4.7 on page 204
2020-12-16	Initial release of 6.4.4.
2021-01-14	Added Liveness detection support for VMware NSX-T service 6.4.4 on page 190.
2021-02-10	Added FortiExtender 6.4.2 dataplan and two modems support for FortiManager 6.4.4 on page 191 and FortiSwitch Manager device monitoring usability improvements 6.4.4 on page 188.
2020-10-22	Initial release of 6.4.3.
2020-10-24	Added Support FortiSOAR license update in an air-gapped environment (closed network) 6.4.3 on page 162.
2020-10-26	Added Workspace Mode can be set per-ADOM 6.4.3 on page 165. Added Policy Hit Count on unused policy 6.4.3 on page 201.
2020-11-02	Added New management extension - FortiAuthenticator added to FortiManager 6.4.3 on page 169.
2020-11-04	Updated information for SD-WAN Orchestrator in Licenses for management extension applications on page 67.
2020-11-17	Added Management extension logs can be accessed in FortiManager or forwarded to FortiAnalyzer to analyze them further 6.4.3 on page 172.
2020-08-06	Initial release of 6.4.2.
2020-08-10	Added SDN connector for Cisco ACI northbound API integration 6.4.2 on page 52.
2020-08-31	Added IPS signature activation filter: hold-time and CVE pattern 6.4.2 on page 136.
2020-09-10	Added Display RSSI signal information and connection status for a managed FortiExtender 6.4.2 on page 139.
2020-06-15	Initial release of 6.4.1.
2020-06-26	Added Updated Security Rating Report 6.4.1 on page 115
2020-07-14	Added FortiSwitch GUI enhancements 6.4.1 on page 100. Added New SD-WAN zone with support for virtual-wan-link and FortiOS 6.4.1 on page 15.
2020-07-20	Added ADOM locking for FortiGates with multiple VDOMs used in multiple ADOMs 6.4.1 on page 118.

Date	Change Description
2020-04-09	Initial release of 6.4.0.
2020-04-15	Added Licenses for management extension applications on page 67. Added Extended SSL and certificate support in ssl-ssh-profile on page 10.
2020-04-23	Added Central SD-WAN, FortiAP, and FortiSwitch templates included in ADOM revision on page 93.
2020-05-08	Added FortiManager support for FortiGate-7000E and FortiCarrier-7000E families on page 95.
2021-05-05	Updated Policy Hit Count on unused policy 6.4.3 on page 201.
2021-06-30	Updated New management extension - FortiPortal added to FortiManager 6.4.4 on page 172.
2022-11-15	Updated Interface-based shaping profiles and monitoring on page 73.

FortiManager 6.4 New Features Guide

This document describes the new features added to FortiManager 6.4. The FortiManager new features are organized into the following categories:

Security-driven Networking

This section lists the new features added to FortiManager for Security-driven Networking. They are organized into the following sections:

NGFW

This section lists the new features added to FortiManager for Next Generation Firewall (NGFW).

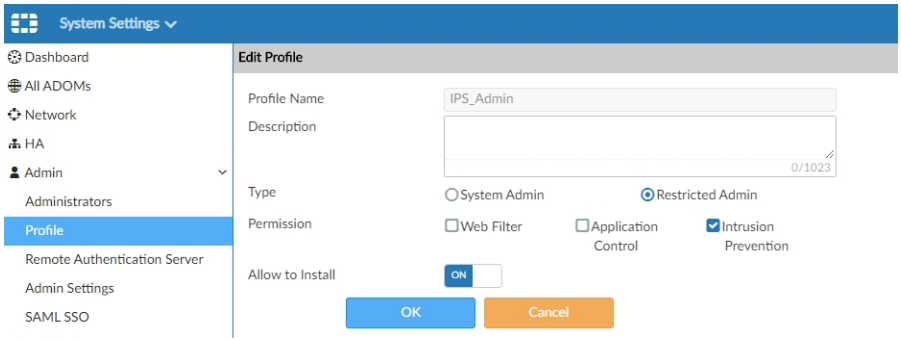
List of new features:

Restricted IPS Admin Profile

The restricted IPS admin profile feature helps customers who are transitioning from dedicated IPS solutions to Fortinet products. This feature provides replacement functions for IPS administrations.

To setup a Restricted IPS Admin Profile:

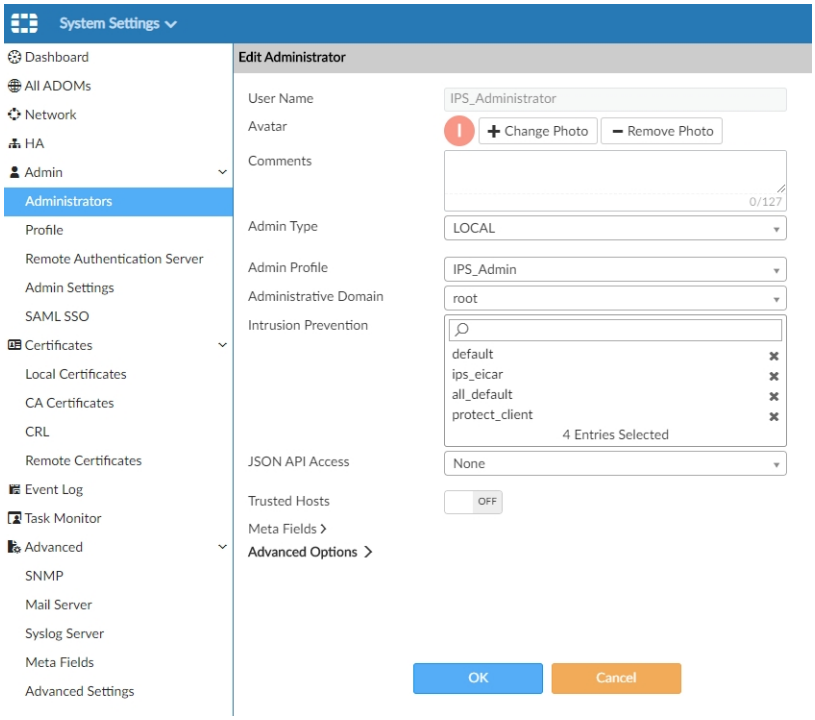
1. Go to *System Settings*. In the tree menu, select *Profile*. Click *Create New* to create an admin profile with its type as *Restricted Admin*.
2. Now, select the admin profile and click *Edit* from the toolbar. Alternatively, you can double-click on the admin profile to edit.
   The *Edit Profile* pane is displayed.



   Toggle *ON/OFF Allow to Install* to enable or disable "Install" permission for the restricted admin. Click *OK*.

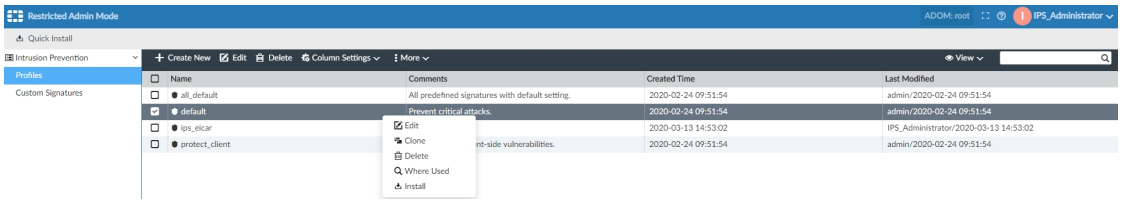
   By default, *Allow to Install* is *ON*. When it is *OFF*, IPS admin can only make IPS config changes and has no permission to push config changes down to FortiGate.

3. In the tree menu, select *Administrators*. Click *Create New* from the toolbar to create an administrator.
4. Select the administrator and click *Edit* from the toolbar. Alternatively, you can double-click on the administrator to edit.
   The *Edit Administrator* pane opens.

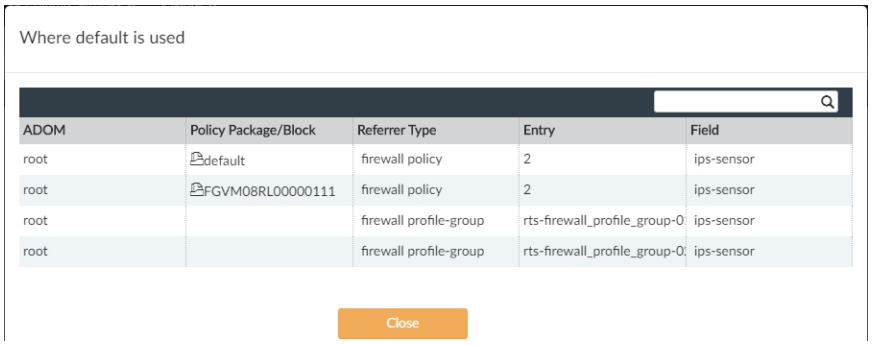


5. In the *Edit Administrator* window, select profiles for permissions and click *OK*.

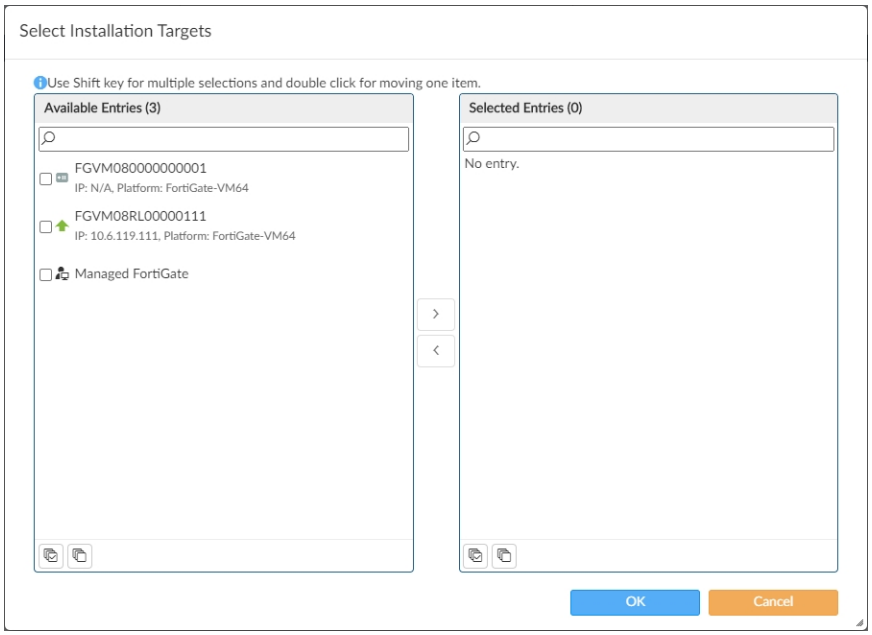
6. Log in with your IPS admin credentials. Go to *Intrusion prevention* > *Profiles* and *Custom Signatures*. IPS admin is able to create, edit, or delete IPS profiles and custom signatures.
7. Select a profile and right-click, select either *Install* or *Where Used*.



Where used dialog shows where the selected profile is being used. Click *Close*.



Select *Install* to select target devices. This copies the profile to the device db, and then installs it to the selected device. Click *OK*.



Extended SSL and certificate support in ssl-ssh-profile

FortiManager includes extended SSL and certificate support in `ssl-ssh-profile`.

Before the extended support, the CLI provided the following support:

`invalid-server-cert` - Allow or block the invalid SSL session server certificate.

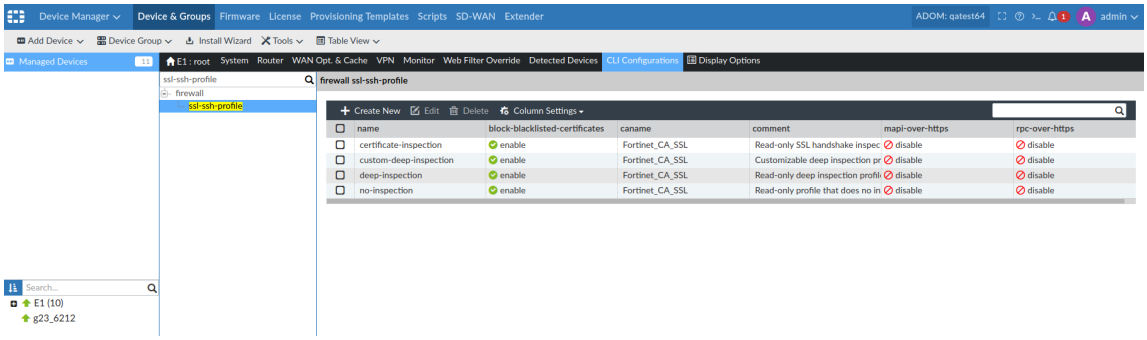
`untrusted-server-cert` - Allow, ignore, or block the untrusted SSL session server certificate.

After the extended support was added, the CLI provides the following options:

```
unsupported-ssl-cipher [allow* | block]
unsupported-ssl-negotiation [allow* | block]
expired-server-cert [allow| ignore | block*]
revoked-server-cert block [allow| ignore | block*]
cert-validation-timeout [allow*| ignore | block]
cert-validation-failure [allow| ignore | block*]
```

To use the extended support in the GUI:

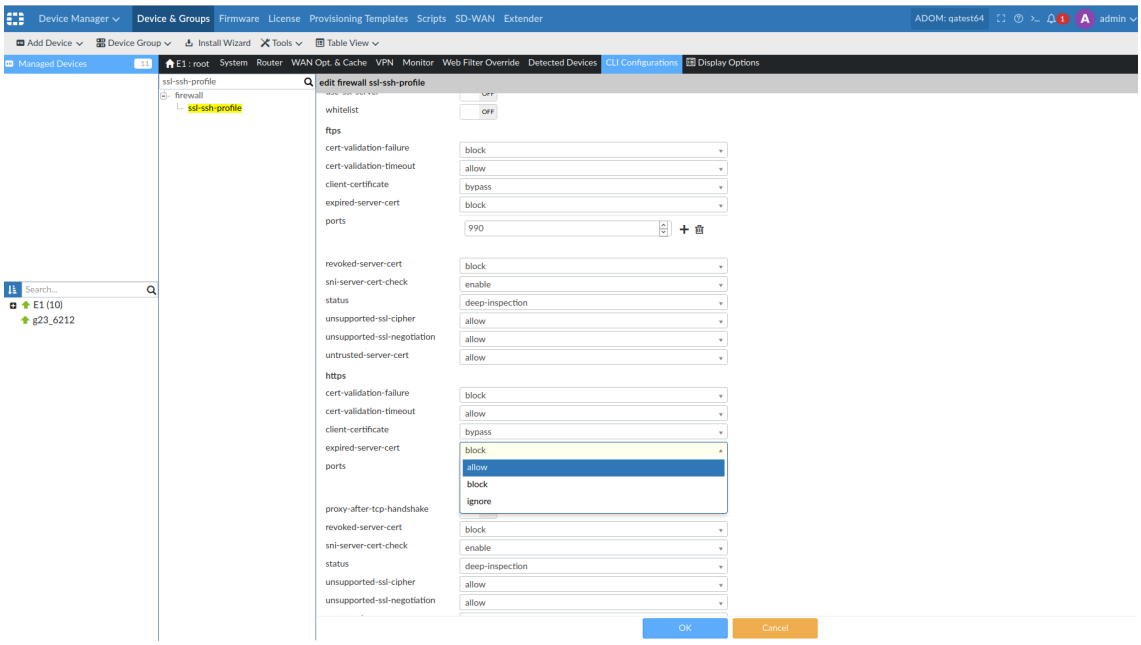
1. Go to *Device Manager* > *Device & Groups*, and display the dashboard for a device.
   a. In the tree menu, select the device group, for example, *Managed Devices*.
      The list of devices display in the content pane and in the bottom tree menu.
   b. In the bottom tree menu, select a device.
      The *System: Dashboard* for the device displays in the content pane.
2. If the *CLI Configurations* menu is hidden, click *Display Options*, and select *CLI Configurations*.
   The CLI Configurations menu is displayed.
3. In the search box, type `ssl-ssh-profile`, and then select the profile.
   The *firewall* > *ssl-ssh-profile* is displayed.



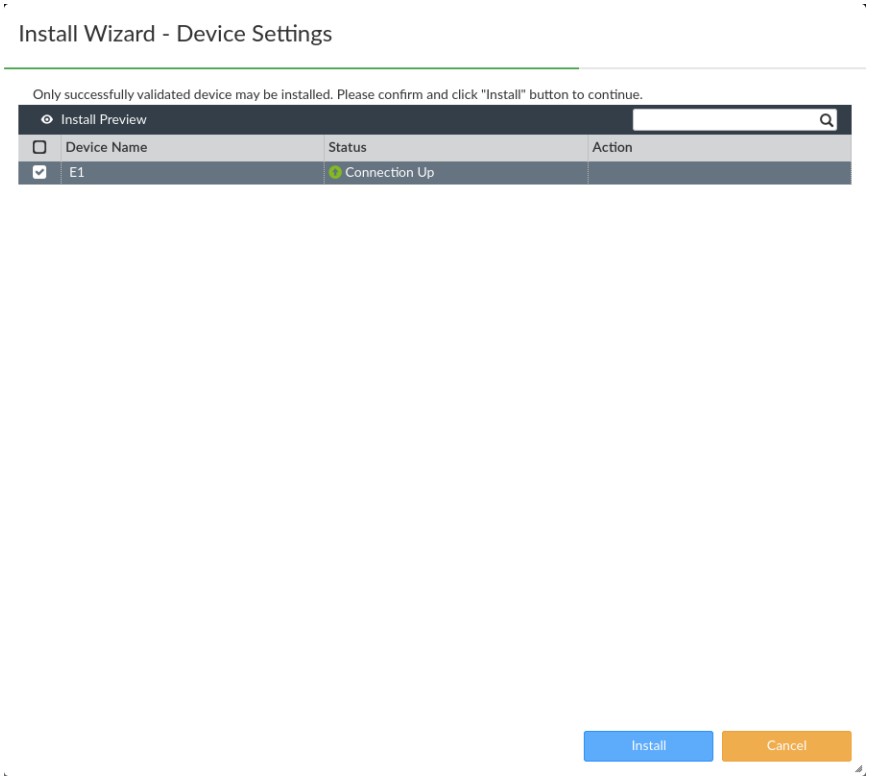
4. Select the checkbox beside *custom-deep-inspection*, and click *Edit*.
   The *firewall* > *ssl-ssh-profile* options are displayed.
5. Scroll down to the *https* section, and view the following new options:

```
unsupported-ssl-cipher [allow* | block]
unsupported-ssl-negotiation [allow* | block]
expired-server-cert [allow| ignore | block*]
revoked-server-cert block [allow| ignore | block*]
cert-validation-timeout [allow*| ignore | block]
cert-validation-failure [allow| ignore | block*]
```

6. In the *expired-server-cert* list, select *allow*.



7. In the *unsupported-ssl-cipher* list, select *block*.
8. Click *OK* to apply the changes.
9. Install the changes to the FortiGate device.



The changes are installed to the FortiGate. You can view the changes on the FortiGate unit by using the CLI.

```
E1 (root) # config firewall ssl-ssh-profile

E1 (ssl-ssh-profile) # edit custom-deep-inspection

E1 (custom-deep-insp~ion) # config https

E1 (https) # show
config https
    set ports 443
    set status deep-inspection
    set unsupported-ssl-cipher block
    set expired-server-cert allow
end

E1 (https) # get
ports                : 443
status               : deep-inspection
proxy-after-tcp-handshake: disable
client-certificate   : bypass
unsupported-ssl-cipher: block
unsupported-ssl-negotiation: allow
expired-server-cert  : allow
revoked-server-cert  : block
untrusted-server-cert: allow
cert-validation-timeout: allow
cert-validation-failure: block
sni-server-cert-check: enable
```

To use the extended support in the CLI:

```
config firewall ssl-ssh-profile
   edit "custom-deep-inspection"
      set comment "Customizable deep inspection profile."
      config ssl
         set inspect-all disable
      end
      config https
         set ports 443
         set status deep-inspection
         set proxy-after-tcp-handshake disable
         set client-certificate bypass
         set unsupported-ssl-cipher allow <-- New
         set unsupported-ssl-negotiation allow <-- New
         set expired-server-cert block <-- New
         set revoked-server-cert block <-- New
         set untrusted-server-cert allow
         set cert-validation-timeout allow <-- New
         set cert-validation-failure block <-- New
         set sni-server-cert-check enable
      end
```

```
    next
end
```

SD-WAN

This section lists the new features added to FortiManager for SD-WAN.

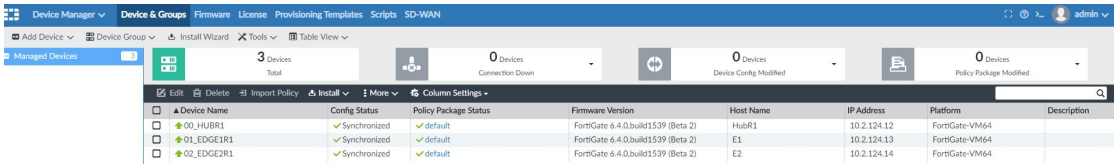
List of new features:

Backup and restore FortiManager settings including SD-WAN Orchestrator configuration

FortiManager has a backup and restore option in *System Settings* pane. If the customer has enabled the SD-WAN Orchestrator docker (one of the tiles under the Management Extensions modules), which is a separate application running on FortiManager, the FortiManager backup includes the configuration for SD-WAN Orchestrator too.

To check the configuration status in Device Manager:

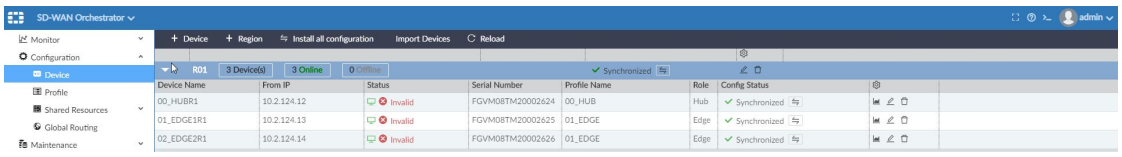
1. Go to *Device Manager* > *Device and Groups*.
2. In the tree menu, select *Managed Devices*.
   The *Managed Devices* pane opens.



   The *Managed Devices* pane shows the configuration status of the devices.

To check the configuration status in SD-WAN Orchestrator:

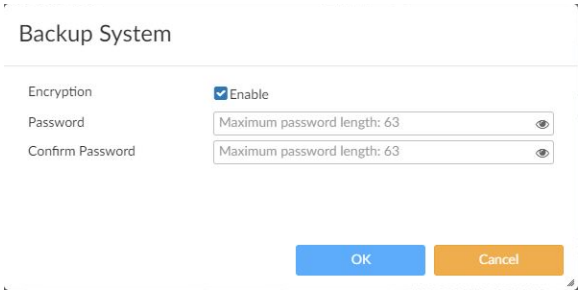
1. Go to *SD-WAN Orchestrator* > *Configuration*.
2. In the *Configuration* dropdown list, select *Device*.
   The *Device* pane opens.



   The *Device* pane shows the configuration status of the devices.

To backup FortiManager settings and SD-WAN Orchestrator configuration:

1. Go to *System Settings* > *Backup System*.
   The *Backup System* dialog opens.



2. In the *Backup System* dialog box, select the *Enable* checkbox to enable encryption and enter/ confirm your password.
   Click *OK*.
   After restoring the backup file, SD-WAN Orchestrator can show the previously configured data.

To backup and restore via the CLI:

1. To backup settings:
   `execute backup all-settings ftp <ip:port> Path/filename <username> <password>`
2. To restore settings:
   `execute restore all-settings ftp <ip:port> Path/filename <username> <password>`

New SD-WAN zone with support for virtual-wan-link and FortiOS - 6.4.1

FortiManager 6.4.1 and later supports SD-WAN zones and the `virtual-wan-link` option available in FortiOS 6.4.1 and later. Each SD-WAN interface member is assigned to a zone. The default zone is named `virtual-wan-link`.

With the implementation of SD-WAN zones, you can no longer select SD-WAN interface members in policies. Instead you must select zones in policies.

After upgrading to FortiManager 6.4.1, an SD-WAN zone named `upg-zone-<interface-name>` is automatically created for each interface member, and affected policies are automatically updated.

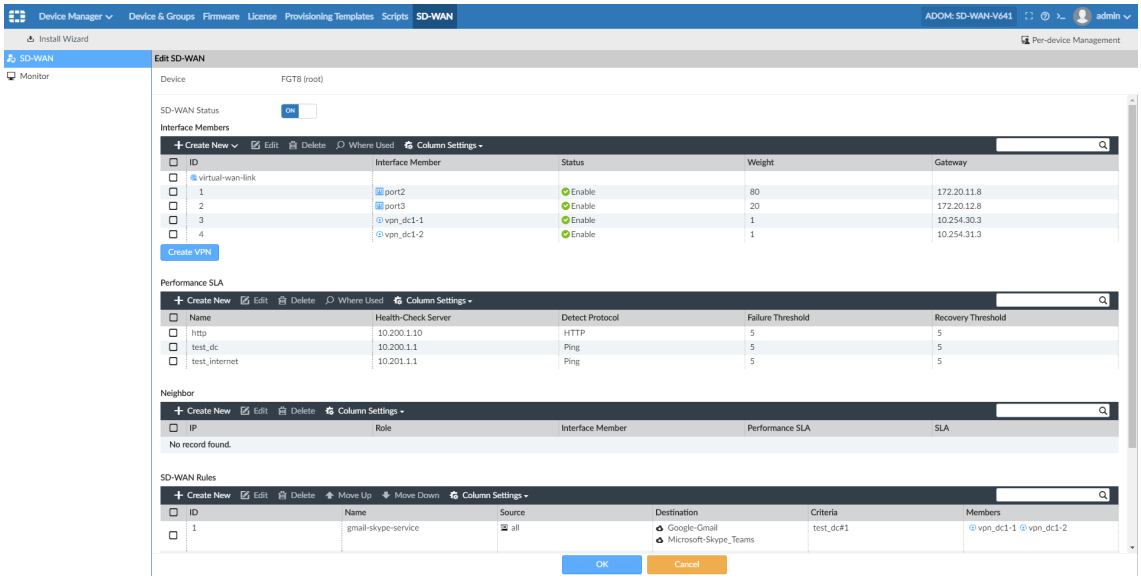
When central management is enabled for SD-WAN in FortiManager, a normalized interface is automatically created when you create an SD-WAN zone.

When you import an SD-WAN zone to FortiManager, FortiManager automatically creates a normalized interface and adds per-device mappings.

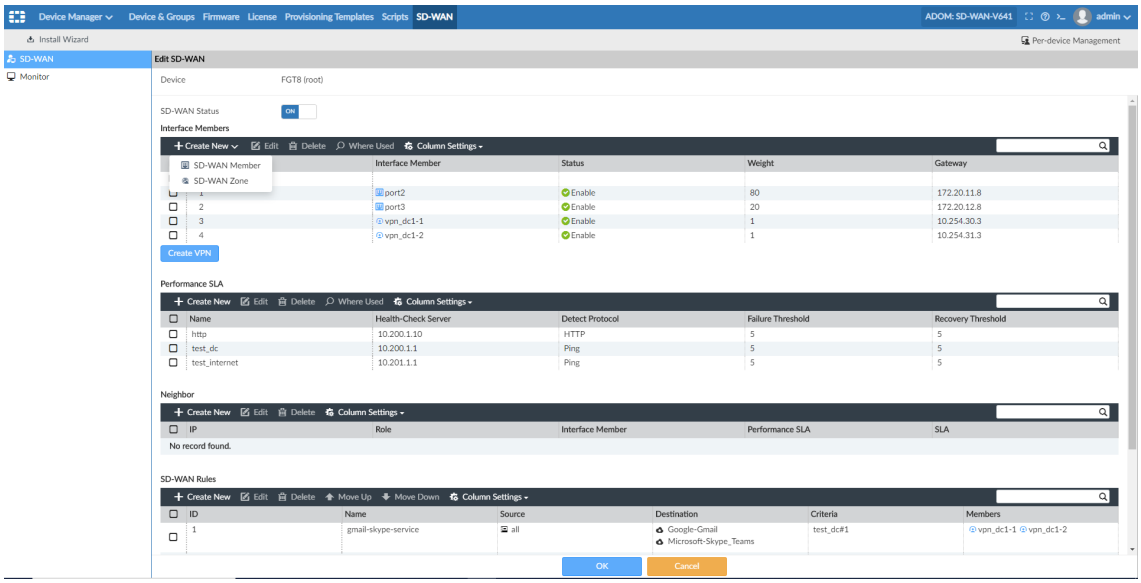
This topic includes the following sections:

Per-device management

When per-device management is enabled in FortiManager, the default SD-WAN zone is named `virtual-wan-link`.



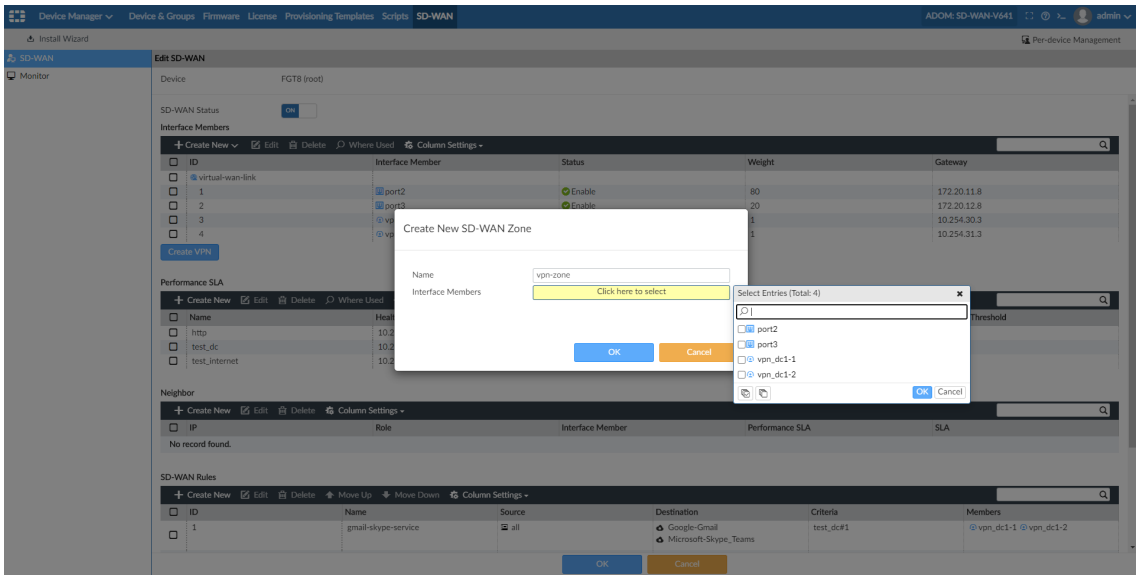
You can create an SD-WAN interface member and an SD-WAN zone:



To create an SD-WAN zone:

1. In an ADOM with per-device management enabled, go to *Device Manager* > *SD-WAN* > *SD-WAN*.
   The SD-WAN configurations are displayed in the content pane.
2. Double-click a configuration to open it for editing, or click *Create New*.
   The SD-WAN settings are displayed.
3. In the *Interface Members* section, click *Create New* > *SD-WAN Zone*.
   The *Create New SD-WAN Zone* dialog box is displayed.
4. In the *Name* box, type a name for the zone.

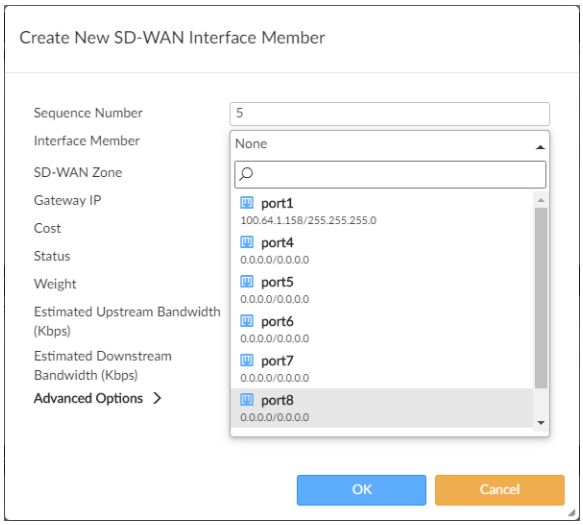
5. Click the *Interface Members* box.
   The list of interfaces is displayed.



6. Select the interfaces to be members of the zone, and click *OK*.
7. Click *OK* to finish creating the zone.

To create an SD-WAN interface member:

1. In an ADOM with per-device management enabled, go to *Device Manager* > *SD-WAN* > *SD-WAN*.
   The SD-WAN configurations are displayed in the content pane.
2. Double-click a configuration to open it for editing, or click *Create New*.
   The SD-WAN settings are displayed.
3. In the *Interface Members* section, click *Create New* > *SD-WAN Member*.
   The *Create New SD-WAN Interface Member* dialog box is displayed.

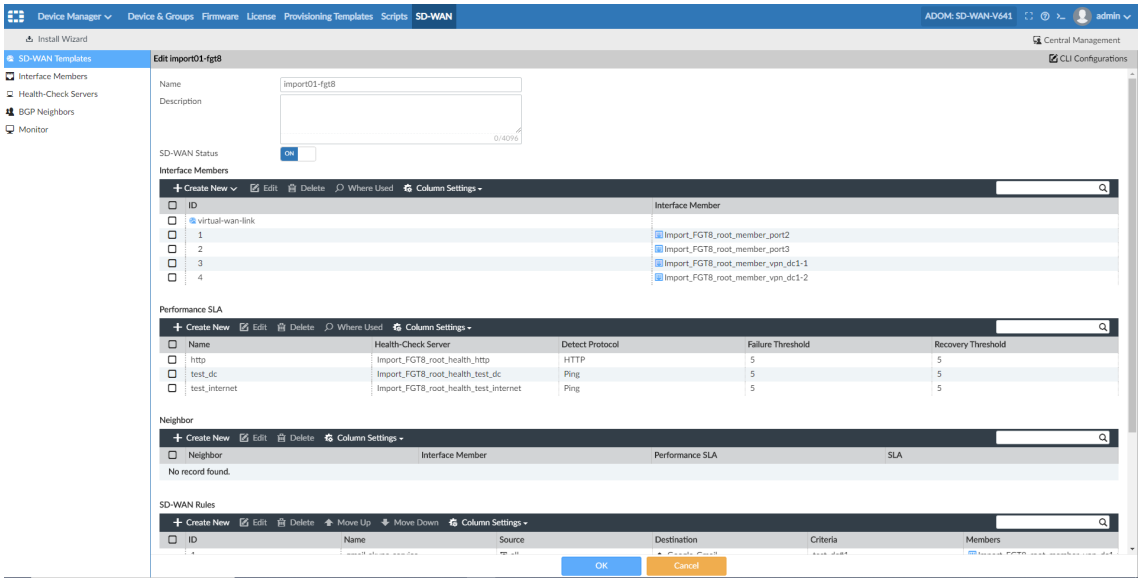


4. Click the *Interface Members* box, and select an interface.
5. In the *SD-WAN Zone* box, select a zone.

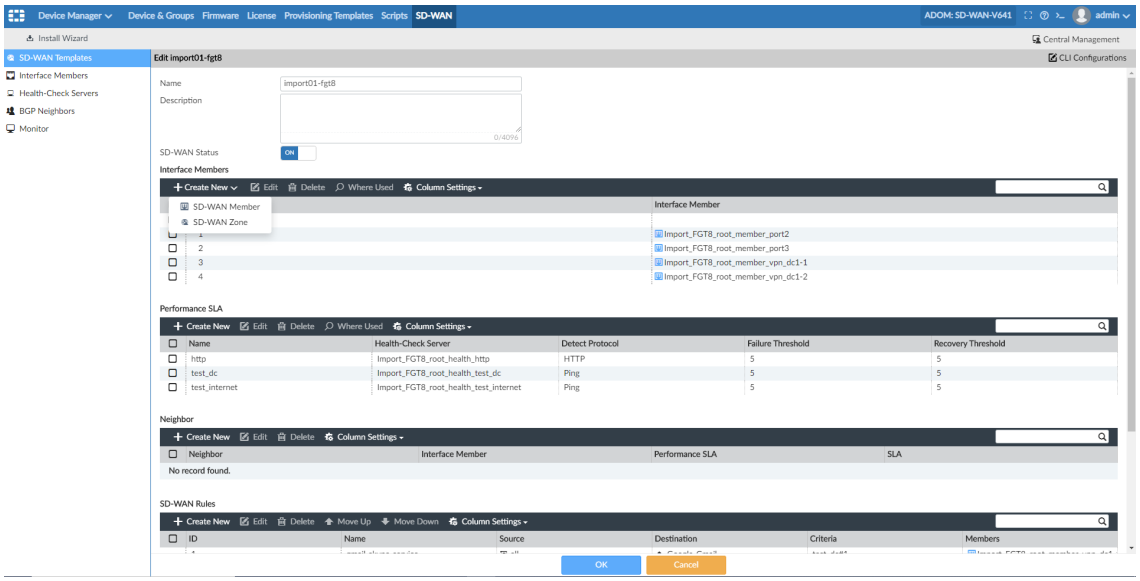
6. Click *OK*.
   The interface is added to the zone.

Central management

When central management is enabled, the default SD-WAN zone is named `virtual-wan-link`.



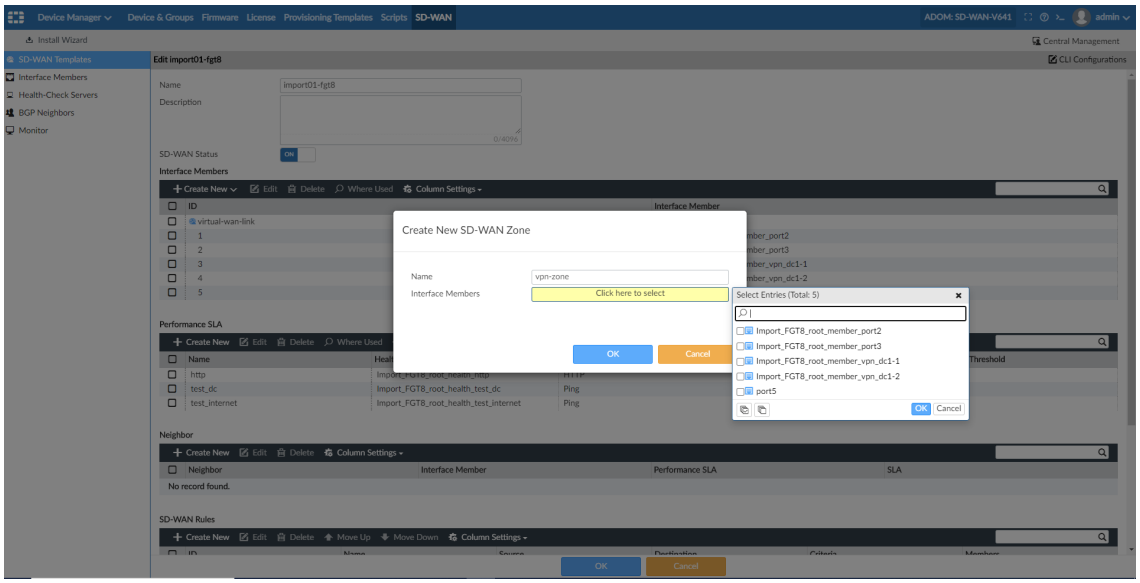
You can create an SD-WAN member and an SD-WAN zone:



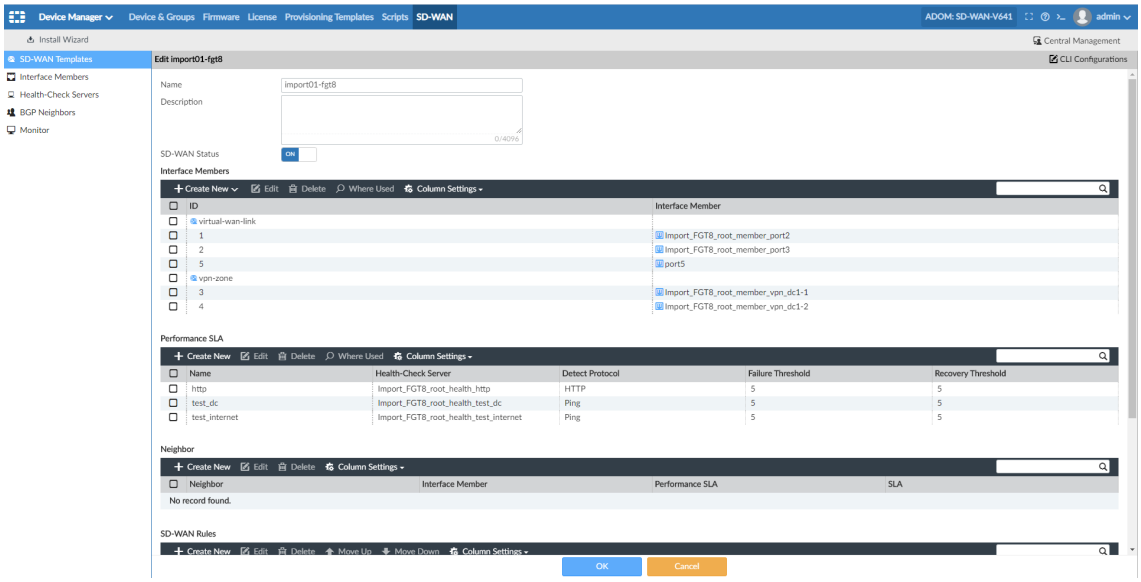
To create an SD-WAN zone:

1. In an ADOM with central management enabled, go to *Device Manager* > *SD-WAN* > *SD-WAN Templates*.
   The templates are displayed in the content screen.

2. Double-click a template to open it for editing, or click *Create New*.
   The SD-WAN settings are displayed.
3. In the *Interface Members* section, click *Create New* > *SD-WAN Zone*.
4. In the *Name* box, type a name for the zone, such as `vpn-zone`.
5. Click the *Interface Members* box.
   The list of interfaces is displayed.



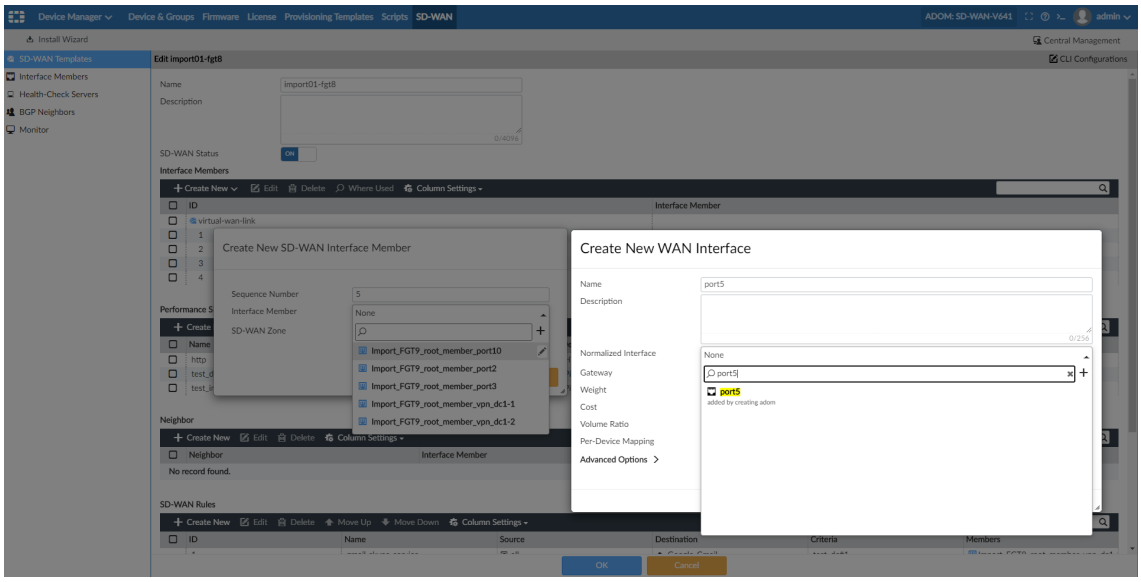
6. Select the interfaces to be members of the zone, and click *OK*.
7. Click *OK* to finish creating the zone.
   In the following example, the zone named *vpn-zone* is created in addition to the default zone named *virtual-wan-link*.



To create an SD-WAN interface member:

1. In an ADOM with central management enabled, go to *Device Manager* > *SD-WAN*.
   The templates are displayed in the content screen.

2. Double-click a template to open it for editing, or click *Create New*.
   The SD-WAN settings are displayed.
3. In the *Interface Members* section, click *Create New* > *SD-WAN Member*.
   The *Create New SD-WAN Interface Member* dialog box is displayed.
4. Create a new SD-WAN interface:
   a. In the *Interface Member* list, click the + icon.
      The *Create New WAN Interface* dialog box is displayed.



   b. In the *Name* box, type a name for the interface.
   c. In the *Normalized Interface*, select an interface.
   d. Complete the remaining options, and click *OK*.
      The SD-WAN interface is created.
5. In the *SD-WAN Zone* box, select the zone.
6. Click *OK*.
   The interface is added to the zone.

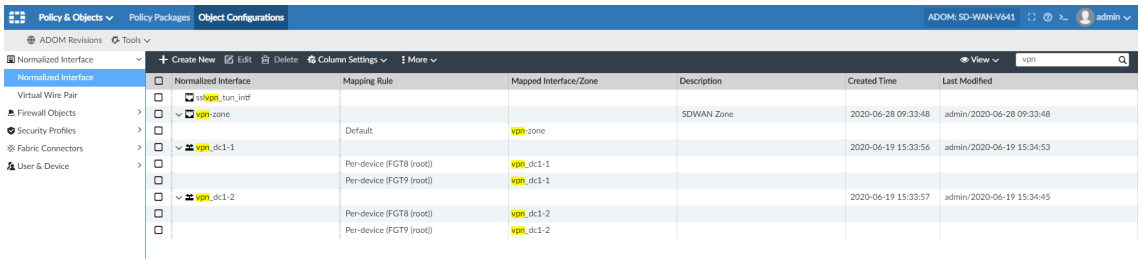
Zones and interface members

You can select SD-WAN zones as source and destination interfaces in firewall policies. You cannot select interface members of SD-WAN zones in firewall policies.

The SD-WAN interface (`virtual-wan-link`) used in policies is replaced by SD-WAN zones.

To view zones and interface members:

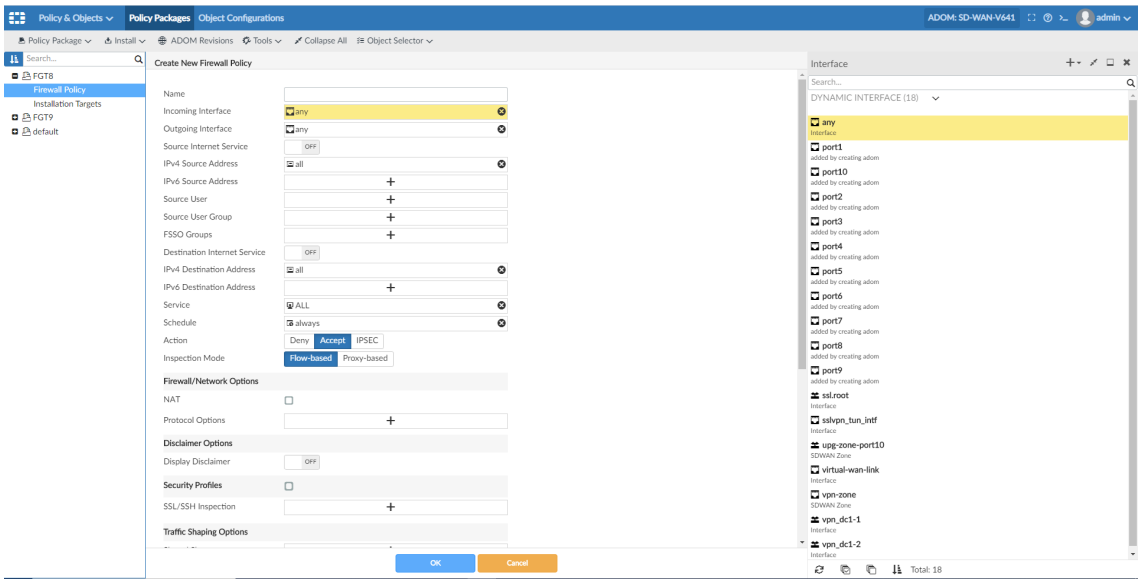
1. Go to *Policy & Objects* > *Object Configuration* > *Normalized Interface*.
   The *Normalized Interface* column displays the name of the interface, and the *Mapped Interface/Zone* column displays the name of the zone.



Zones in firewall policies

To use a zone in a firewall policy:

1. Go to *Policy & Objects* > *Policy Packages* > *Firewall Policy*.
2. In the content pane, click *Create New*.
   The *Create New Firewall Policy* pane is displayed.
3. Click the *Incoming Interface* box, and select a zone.



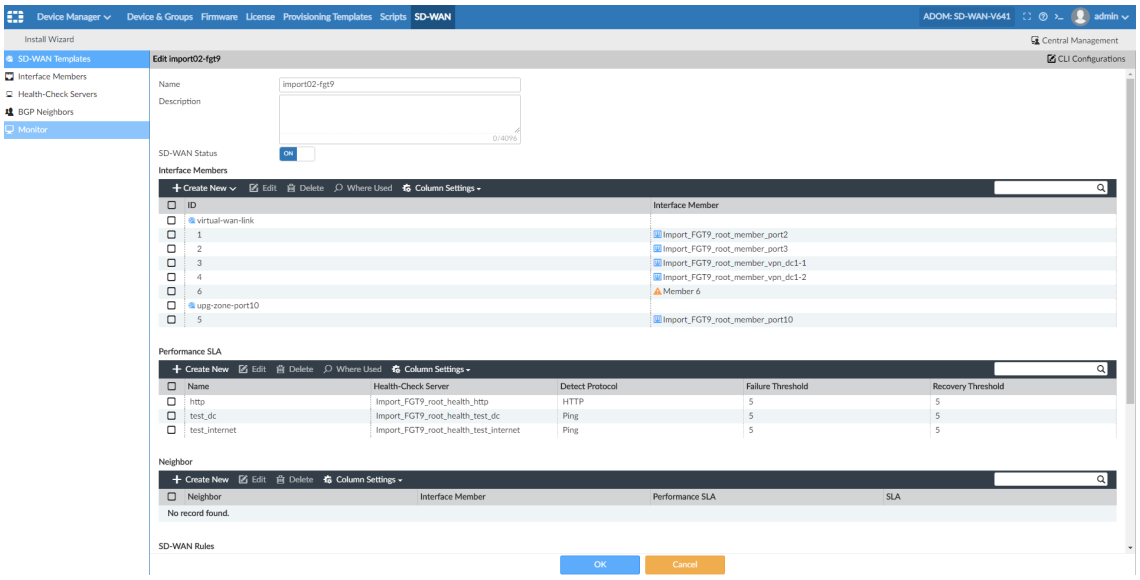
4. Click the *Outgoing Interface* box, and select a zone.
5. Set the remaining options, and click *OK*.

SD-WAN interface members after upgrade

Before FortiManager 6.4.1, you could use SD-WAN interface members directly in a policy. After upgrading to FortiManager 6.4.1, SD-WAN interface members are automatically upgraded to zones. Upgraded SD-WAN members are named *upg-zone-<interface-name>*, and they replace interfaces in policies.

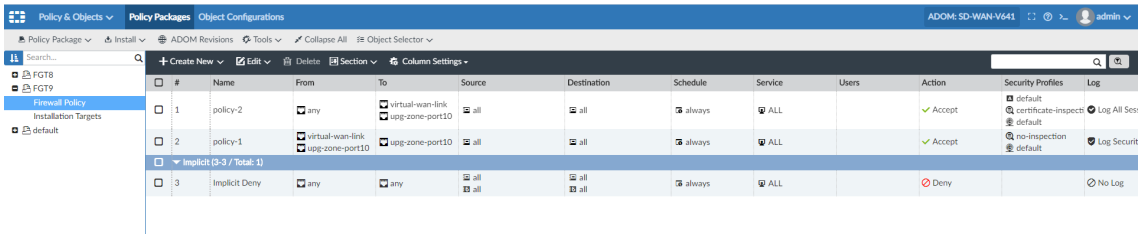
To view SD-WAN members after upgrade:

1. Go to *Device Manager* > *SD-WAN* > *SD-WAN Templates*.
2. Double-click a template to open it for editing.
   The upgraded SD-WAN members are displayed.



To view upgraded SD-WAN members in policies:

1. Go to *Policy & Objects* > *Policy Packages* > *Firewall Policy*.
   The upgraded SD-WAN members are displayed.



Interface widget added to system templates - 6.4.2

System templates now include an *Interface* widget. The *Interface* widget is useful when you want to perform the following actions:

- Create a VLAN interface on top of a physical interface for a large number of FortiGate devices
- Create LAG interfaces
- Configure interface settings such as an IP and DHCP subnet range on a LAN interface
- Create a zone

When you create interface settings for a system template, you can specify which settings can be overridden on each device after the system template is applied. You can also access a preview of the actions per model and device.

In the DNS widget, you can also specify which settings can be overridden.

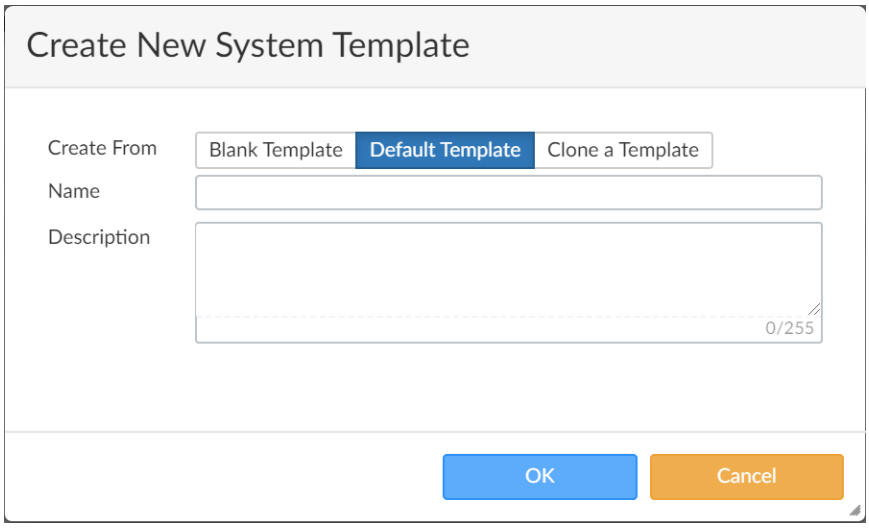
This topic contains the following sections:

Creating system templates with interface actions

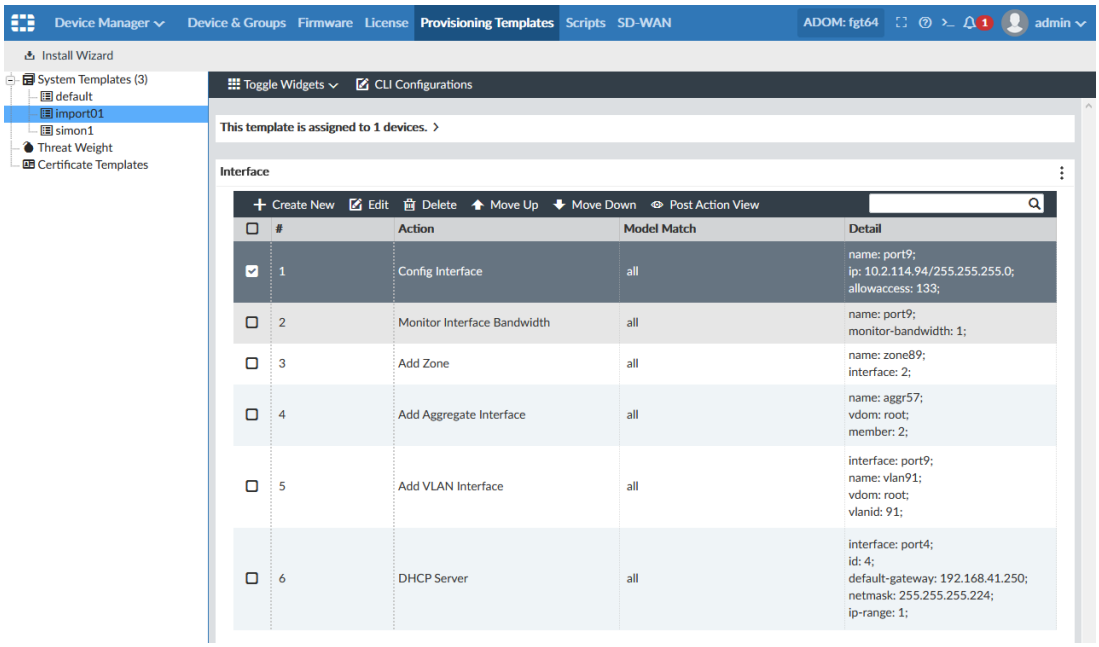
You can now create system templates with interface actions by using the *Interface* widget.

To create a system template with interface actions:

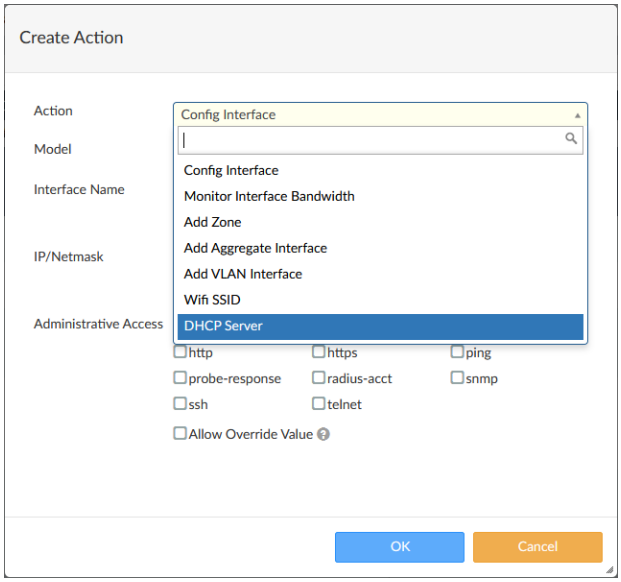
1. Go to *Device Manager* > *Provisioning Templates* > *System Templates*.
2. Create a system template:
   a. Click *Create New*.
   The *Create New System Template* dialog box is displayed.



   b. Beside *Create From*, choose whether to create the template from a *Blank Template*, *Default Template*, or *Clone a Template*.
   c. In the *Name* box type a name for the template, and click *OK*.
   The system template is created.
3. Double-click the system template to open it for editing.
4. From the *Toggle Widgets* list, select *Interface*.
   The *Interface widget* is displayed.



5. Click + *Create New*.
   The *Create Action* dialog box is displayed.



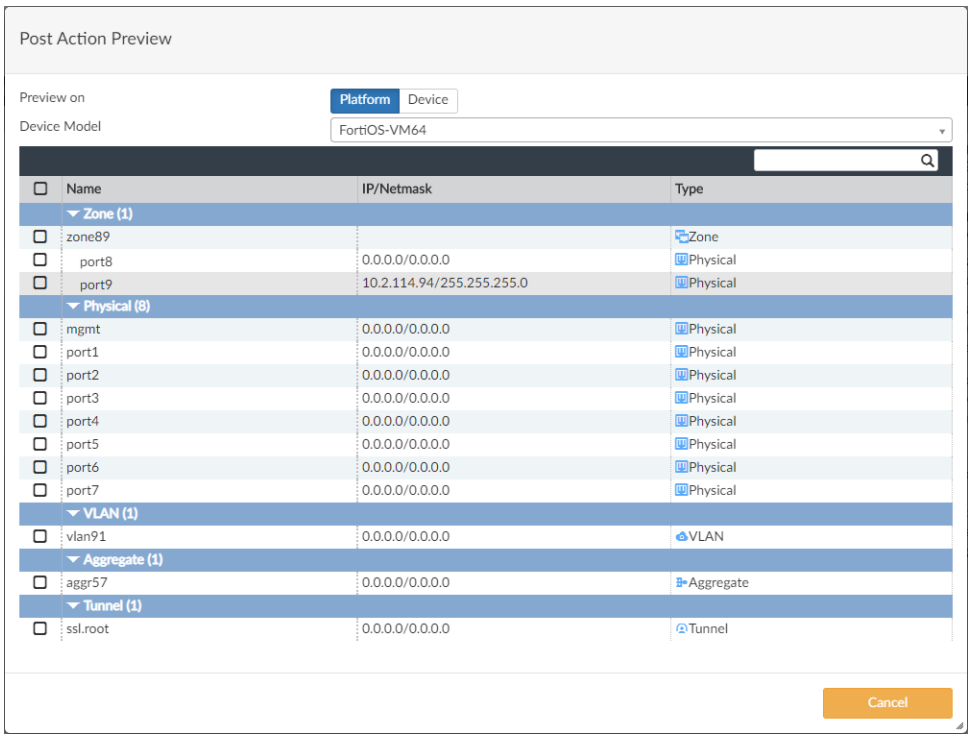
6. In the *Action* list, select an action.
7. Complete the options, and click *OK*.
   The interface action is created.

Accessing a post action preview of interface actions

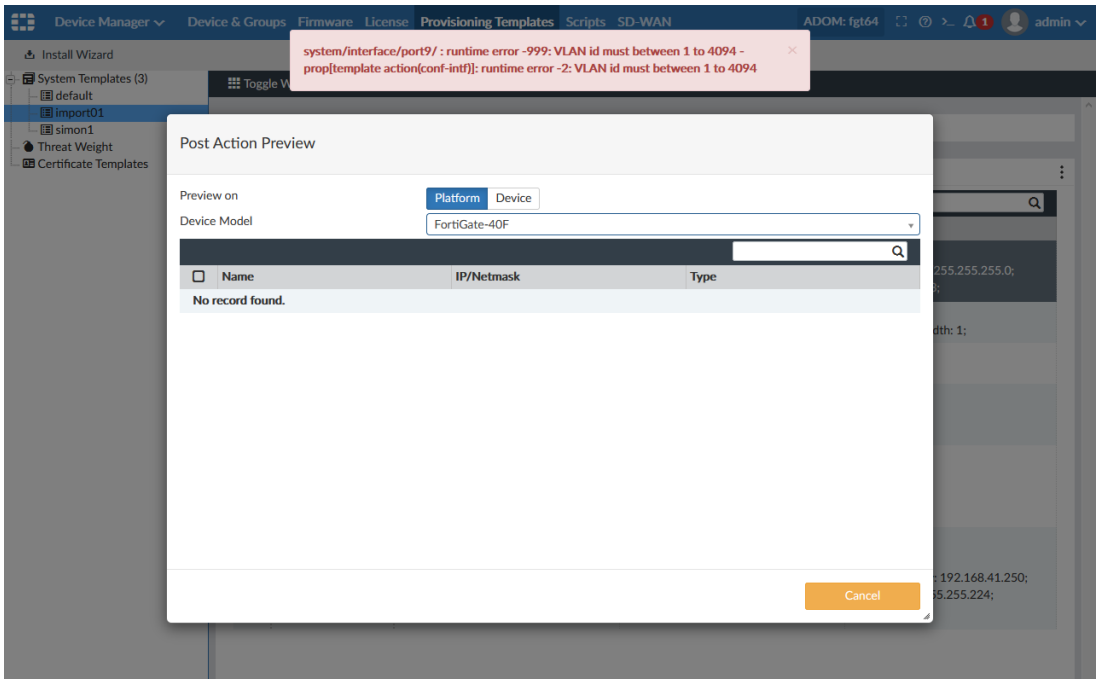
After you create an interface action, you can view a preview of the interface action per model or device.

To access a post action preview:

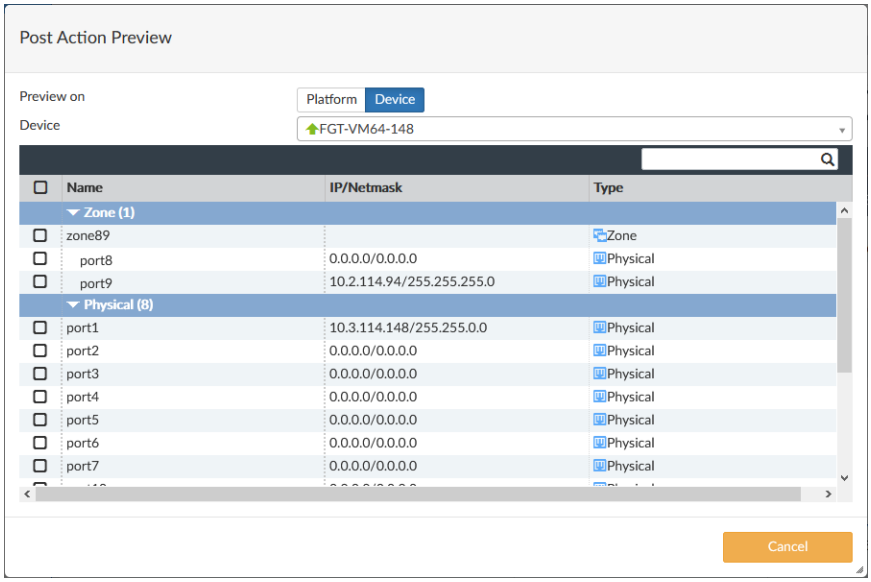
1. Go to *Device Manager* > *Provisioning Templates* > *System Templates*.
2. In the tree menu, select a template with an interface.
   The template details are displayed in the content pane.
3. In the *Interface* widget, select an interface, and click *Post Action View*.
   The *Post Action Preview* dialog box is displayed.
4. Beside *Preview on*, click *Platform* or *Device*, and then select the platform or device from the list.
   In the following example, the selected platform has the same type of port.



In the following example, the selected platform does not have the same type of port, and an error is displayed.



In the following example, the selected device has the same type of port.



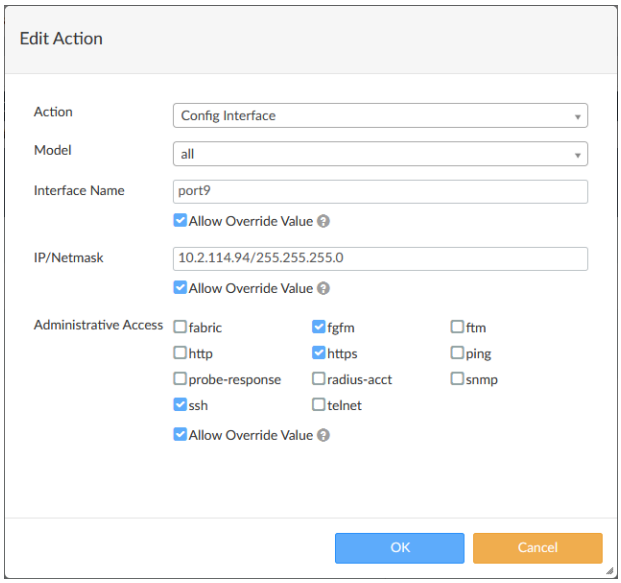
5. Click *Cancel* to close the dialog box.

Allowing system template setting overrides

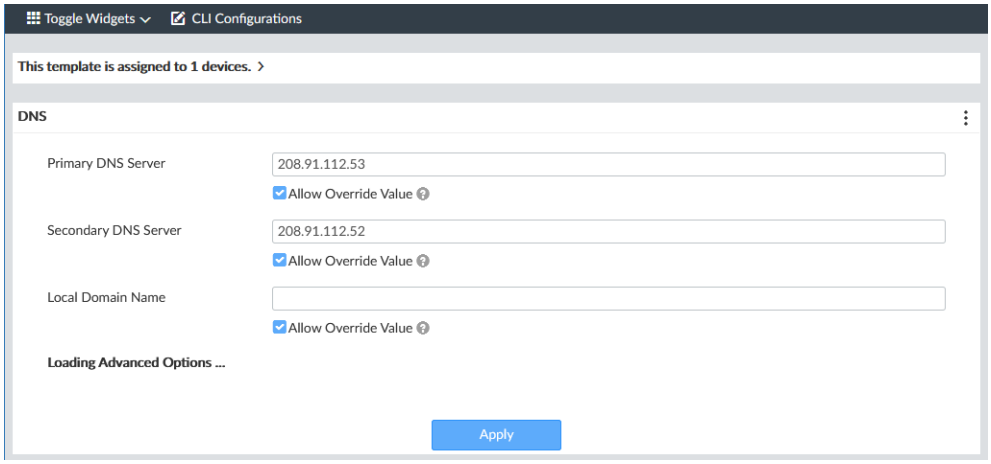
When you create a system template that includes settings from the *Interface* widget or the *DNS* widget, you can allow value overrides. When overrides are allowed, you can change system template settings for each device after the template is applied.

To allow system template overrides:

1. Go to *Device Manager* > *Provisioning Templates* > *System Templates*.
2. Double-click a system template to open it for editing.
3. In the *Interface* widget, double-click an interface to open it for editing.
   The *Edit Action* dialog box is displayed.



4. By the options for which you want to allow overrides, select the *Allow Override Value* checkbox, and click *OK*.
5. In the *DNS* widget, select the *Allow Override Value* checkbox beside the options for which you want to allow overrides.

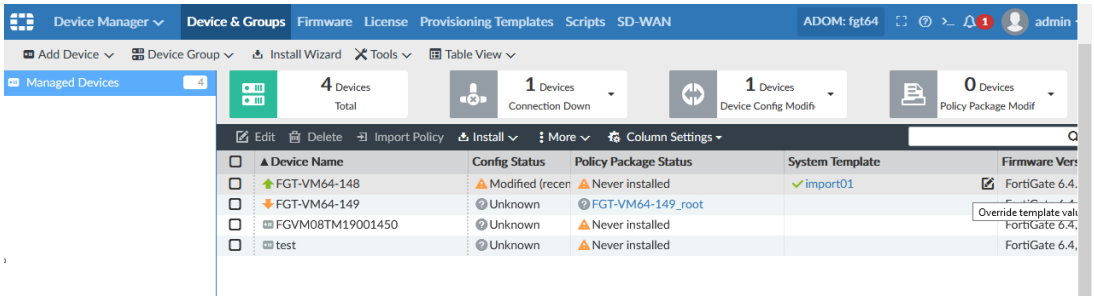


Overriding system template settings

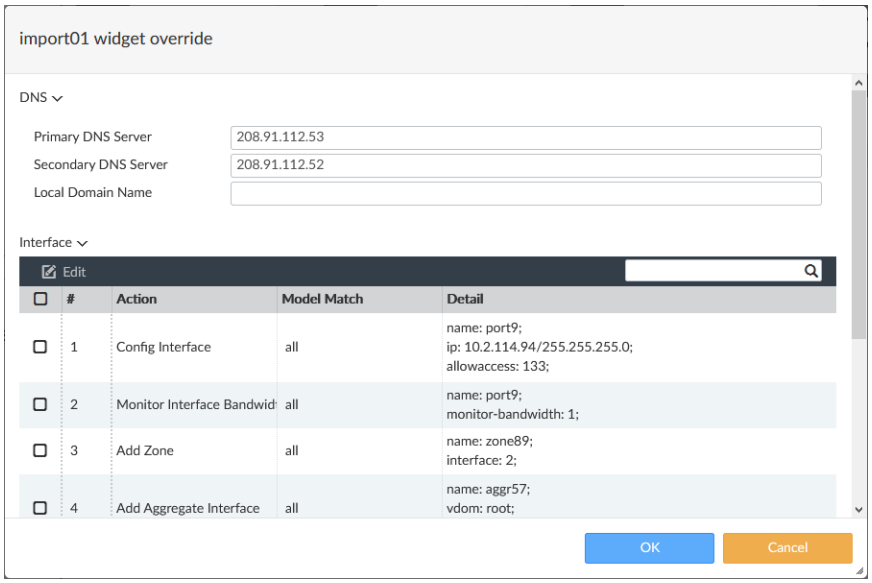
When you create a system template that includes settings from the *Interface* widget or the *DNS* widget, and you have enabled overrides for options, you can override values for each device after the template has been applied.

To override system template settings:

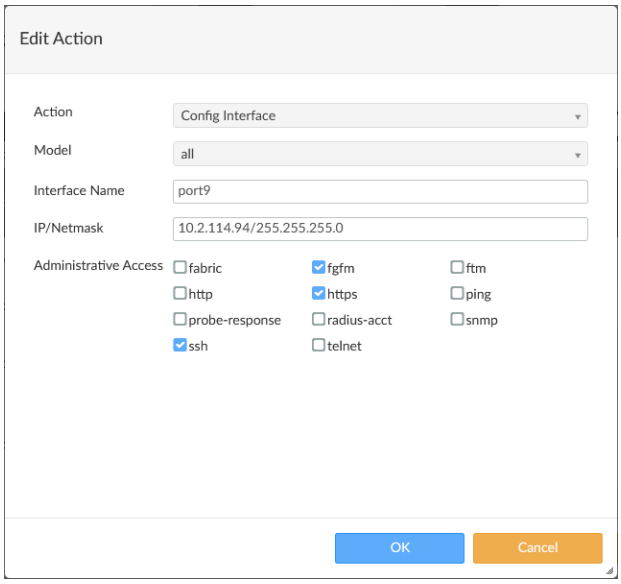
1. Go to *Device Manager* > *Device & Groups* > *Managed Devices*.
2. In the content pane, select a device that uses a system template.
3. In the *System Template* column, hover over the template name.
   An *Override Template Values* icon is displayed.



4. Click the *Override Template Values* icon.
   The system template settings are displayed.



5. For *DNS* settings, edit the options.
6. For *Interface* settings, double-click an action to open it for editing.
   The *Edit Action* dialog box is displayed.



7. Edit the settings, and click *OK*.
   The setting overrides are saved.
8. Click *OK*.

Dynamic Cloud Security

This section lists the new features added to FortiManager for Dynamic Cloud Security. They are organized into the following sections:

Public cloud

This section lists the new features added to FortiManager for public cloud.

List of new features:

Support for cloud-init service for KVM, Azure, and AWS - 6.4.1

You can use the cloud-init service for customizing a prepared image of a virtual installation. The cloud-init service is built into the virtual instances of FortiManager-VM found on the support site so that you can use them on a VM platform that supports the use of the service. To customize the installation of a new FortiManager-VM instance, you must combine the seed image from the support site with user data information customized for each new installation.

Hypervisor platforms such as QEMU/KVM support the use of this service on most major Linux distributions, as well as BSD and Hyper-V. A number of cloud-based environments, such as VMware and AWS also support it.

You can use the cloud-init service to help install different instances based on a common seed image by assigning hostnames, adding SSH keys, and settings particular to the specific installation. You can add other more general customizations, such as the running of post install scripts.

While cloud-init is the service used to accomplish the customized installations of VMs, various other programs, depending on the platform, are used to create the customized ISOs used to create the images that will build the FortiManager-VM.

This topic includes the following sections:

KVM

To configure on KVM:

1. On the host server (Ubuntu), start service `libvirtd`.
2. Prepare the FortiManager configuration and license file.
   This license is named `0000`, without any extension.

The folder structure should be as follows:

```
<holding folder>
/openstack
/content
0000
/latest
user_data
```

For example:

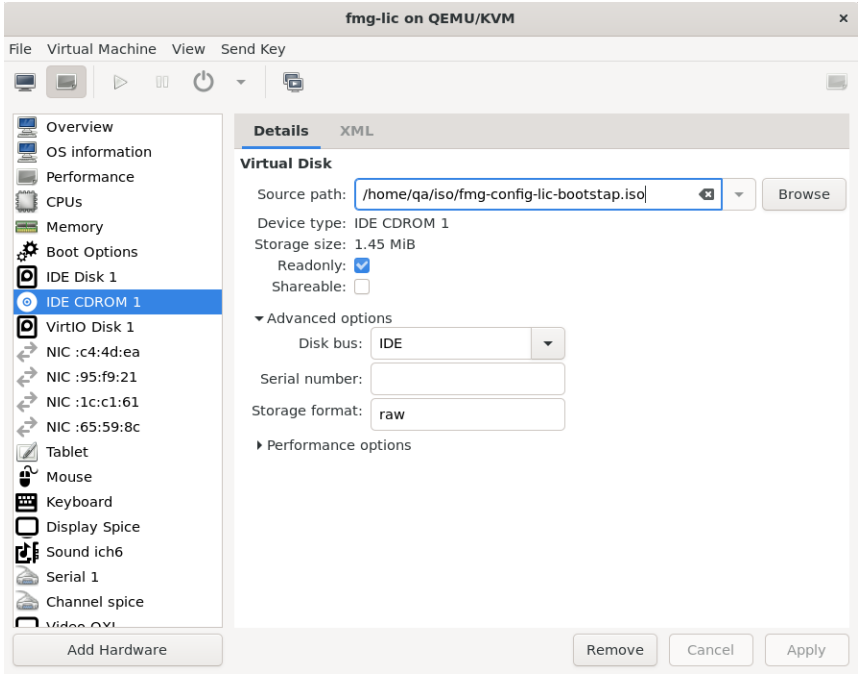
```
config system global
    set hostname fmg-boot-strap
end
```

3. Convert the folder to an ISO image using the mkisofs utility.
Following is the syntax of the command:

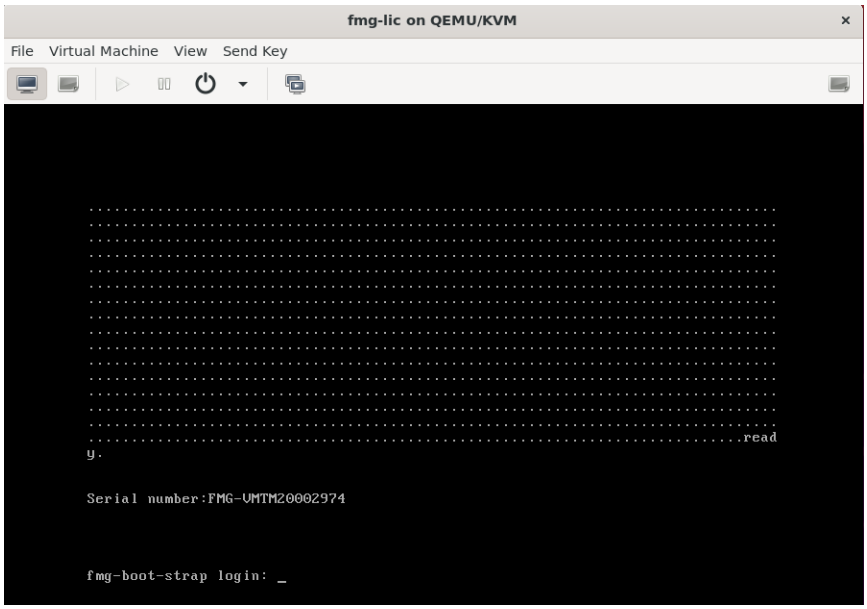
```
mkisofs [options] [-o <filename of new ISO> pathspec [pathspec...]
```

4. Create a FortiManager instance, attach a virtual CDROM, which is based on `fmg-config-lic-bootstap.iso`. The following command sets up a virtual CDROM drive as if it were on an IDE bus holding a virtual CD in it with no cache, and the data is in RAW format.

```
disk /home/username/test/fmg-config-lic-
bootstap.iso,device=cdrom,bus=ide,format=raw,cache=none -
```



5. Boot up the FortiManager KVM virtual machine.
In the following example for FortiManager, the configuration and license upload to the FortiManager KVM virtual machine.

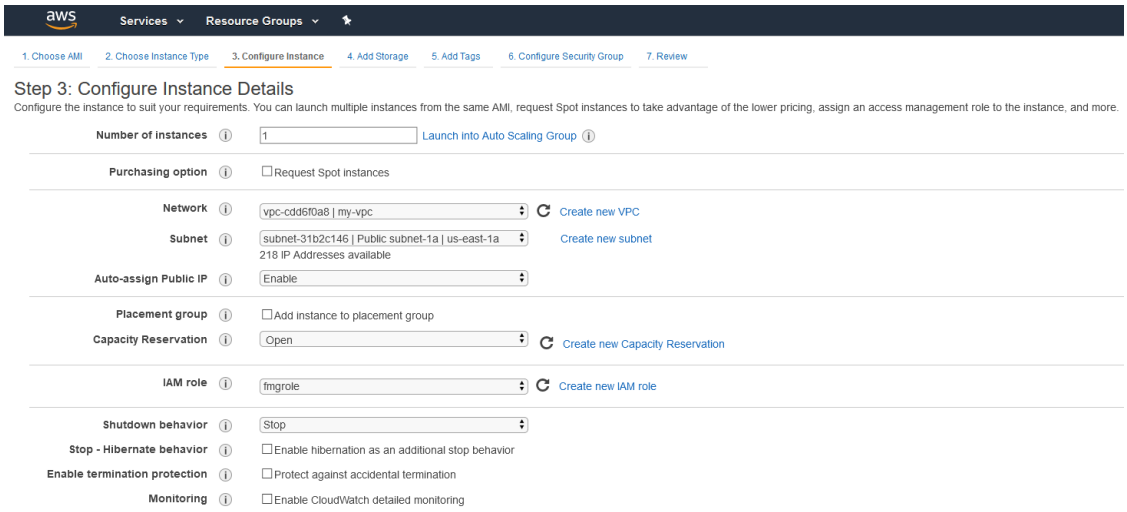



```
bash# cat vmd.log.1
[186] cdrom mounted
[186] /cdrom/openstack/content/0000: size=9171:
-----BEGIN FMG VM LICENSE-----
QAAAAKgh6/7exA+Da/9ho2iypJYLjYKx+vFPBYd6cR6XlTq1WFz95Fz+b1n1sa2OPLldeC5h5sgh
CZMEcGUczbnSZMcQGgAAMC/mTe8EPRK/ARkMpi8Av3IIIcm7Irgds8xk+cgeMpZTMBtq2FrXsAmr
yErFgUgYmouRu9VMtJnJln4nnFRXZzsBez/Xa7XeBBUeHuLuxAiHyI2rIUfXQOPeIgV06eLrFLdu
UpD1EqadFK3eDDoMX4wEFzLHJbbBrjErWKvu2Cf94sEDsaVQmI/Cv5nOZd9rQgR2TdxQ06YO25dr
cRuhoxA/nY4fvqwOcHbhUYpafF2NDeKiXzDVS1iRun5ZYFcCuIOTkGr2AQb5zx6MdlQgc+k8boI0

.......................

JAyU8CgENbH++ClFTDAG6lznT68KcZDF7lcoAr56+p7OjXBEZrwUFVVIv4CWCtfntG1v7uE9Po0P
9PZyNgupzf7lstWtYDfrgSZO
-----END FMG VM LICENSE-----

[186] /cdrom/openstack/latest/user_data: size=438:
config system global
    set hostname fmg-boot-strap
end
```

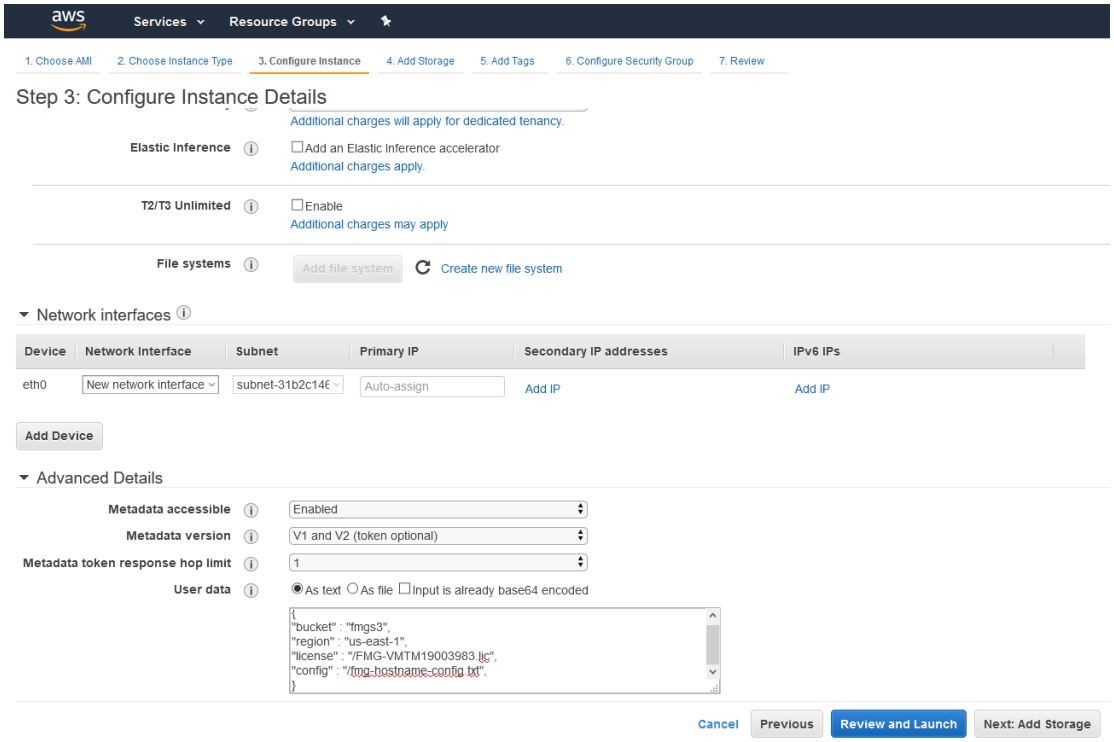
AWS

To configure on AWS:

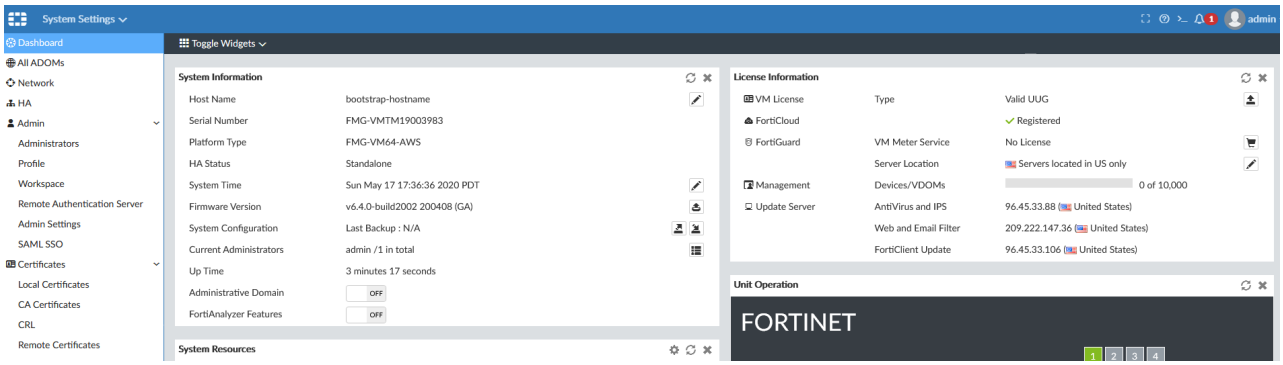
1. Go to the AWS marketplace, and follow the procedure to launch a FortiManager AZURE virtual machine.
2. On the *3. Configure Instance* page, select the VPC subnet and the IAM role.
   When selecting the VPC subnet, select the IAM role that was created, and specify information about the license file and configuration file from the AWS S3 bucket that was previously configured under *Advanced Settings*. In this example, the *IAM role name* is *fmgrole*.



3. Expand *Advanced Details*, and set *User data* to *As text*, for example:



4. Go to the FortiManager GUI, and log in.
5. In FortiManager, go to *System Settings* > *Dashboard*.
   In the following example for FortiManager, the *System Information* widget displays the specified hostname, and the *License Information* widget displays the activated license.



Microsoft Azure

To configure on Microsoft Azure:

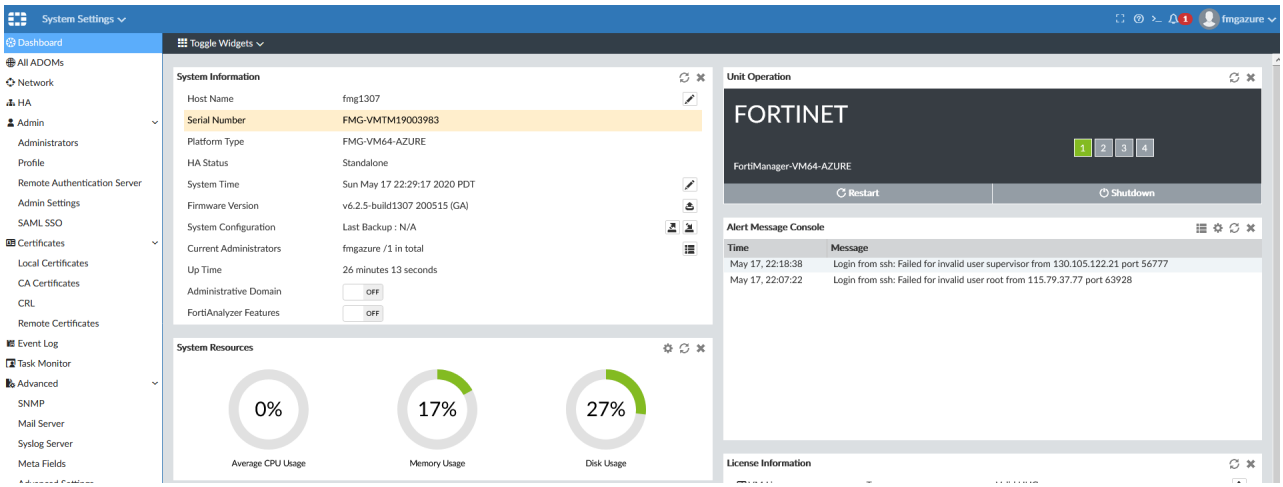
1. Use PowerShell to deploy the FortiManager Azure VM with user data.
2. Create a MIME text file named `azureinit.conf` in local PC `C:\Azure\misc` directory. You can change the directory path and file name using the `$customdataFile = C:\Azure\misc\azureinit.conf` parameter in the `ps1` file. The `azureinit.conf` is the text file in MIME format that includes both FortiGate CLI commands and license file content.

```
Content-Type: multipart/mixed; boundary="==========0740947994048919689=="
MIME-Version: 1.0

--========0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config"

config system admin setting
    set idle_timeout 480
    set shell-access enable
end

--========0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license"

-----BEGIN FMG VM LICENSE-----
QAAAAD1P27eiQC4JGGA1wDYnqMasNcDlXUtjg02/nt21seyucBTncObcRqPsXXFcRqkpoINA83PC
........
IOb6sMYu8MnmDPAJLgygex1BdImccRJ3pe+E9ZgT5tAu7gBVhDa5Bo/kf3IdJOoRdxvFXcUGC0+k
4TgteYmIRK7E5C0ZGV0AGqn2zTmwaFxF9J22R68tkI3fGbhGbAfjcPN5IAdC7TwHWyJWEoOqy8o/
TJ9wReuzEIWC3SrWtgpgfMNM527h4RQrLXBJP0VOm+C4ZHkedrbBy7qFQWhHC+Lps8rsPh/Qj1PN
Ii6kVnHrAgf9dI7C4IAmEKlQ
```

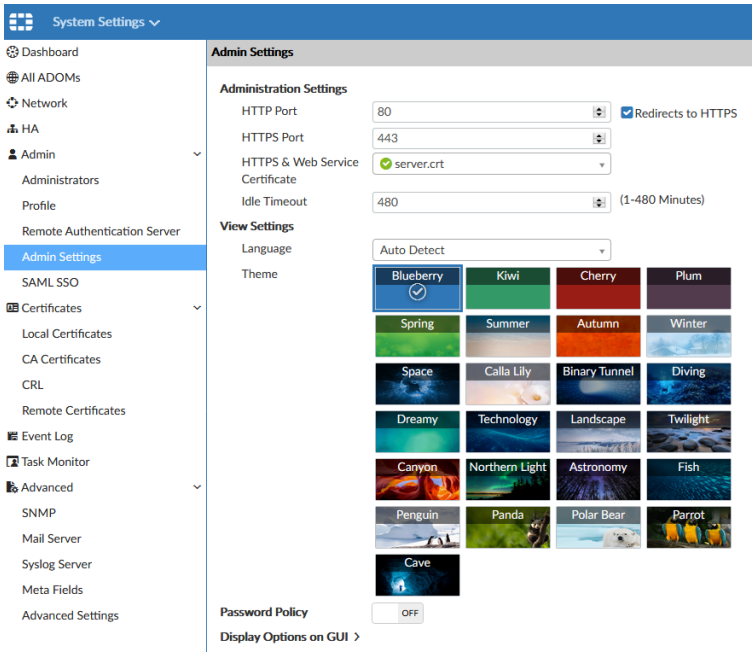
```
-----END FMG VM LICENSE-----

--================0740947994048919689==--
```

After FortiManager Azure VM is created, the FortiManager license and configuration are uploaded.

3. Go to FortiManager GUI, and log in.
4. Go to *System Settings* > *Dashboard*. In the following example, the *System Information* widget displays the serial number.



5. Go to *System Settings* > *Admin* > *Admin Settings*.
The following example displays the *Administration Settings*:



Zero Trust Network Access

This section lists the new features added to FortiManager for Zero Trust Network Access.

List of new features:

Per policy lock

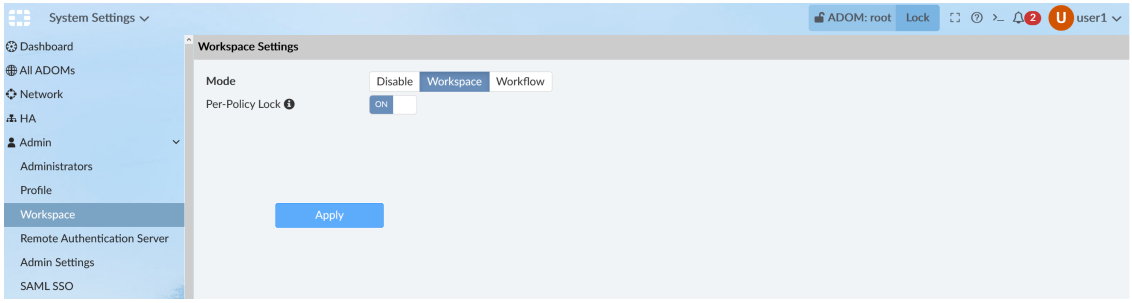
In normal workspace mode, you can lock individual policies.

If you want to modify a policy, you don't need to lock the entire policy package. Once you lock a policy, a padlock icon appears beside the policy. Others are now unable to modify your policy or lock the policy package where the locked policy is located, and unable to lock the ADOM.

If you hover your cursor over the padlock icon, you can see who locked the policy and the time at which it was locked.

To enable per policy lock:

1. Go to *System Settings* > *Workspace*.
   The *Workspace Settings* pane opens.



2. In the *Workspace Settings* pane, select the *Mode* as *Workspace* and enable *Per-Policy lock*.
3. Click *Apply*.

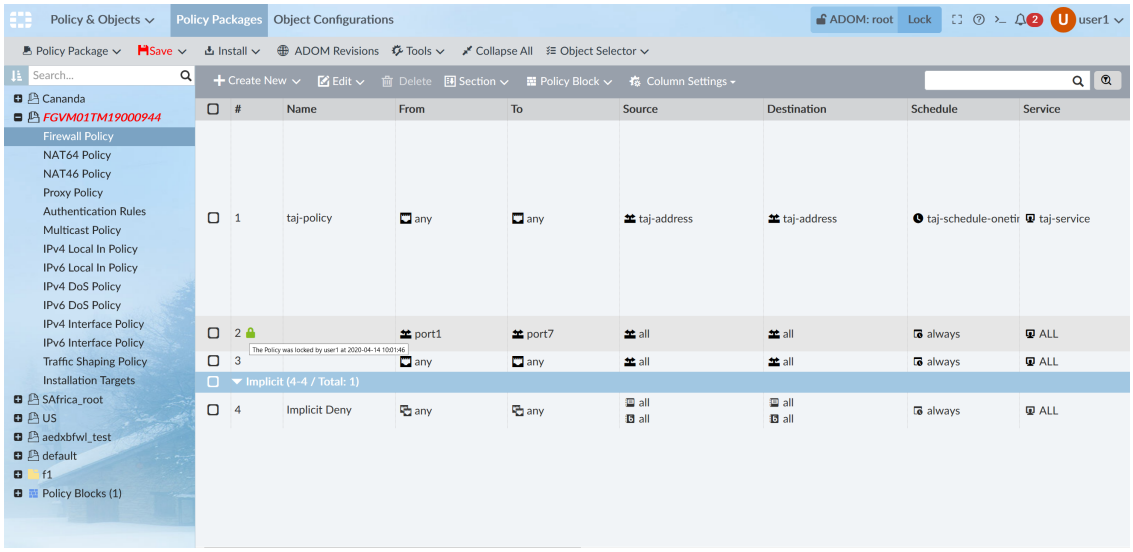
To enable per policy lock via the CLI:

1. In the *CLI Console* widget enter the following CLI commands:

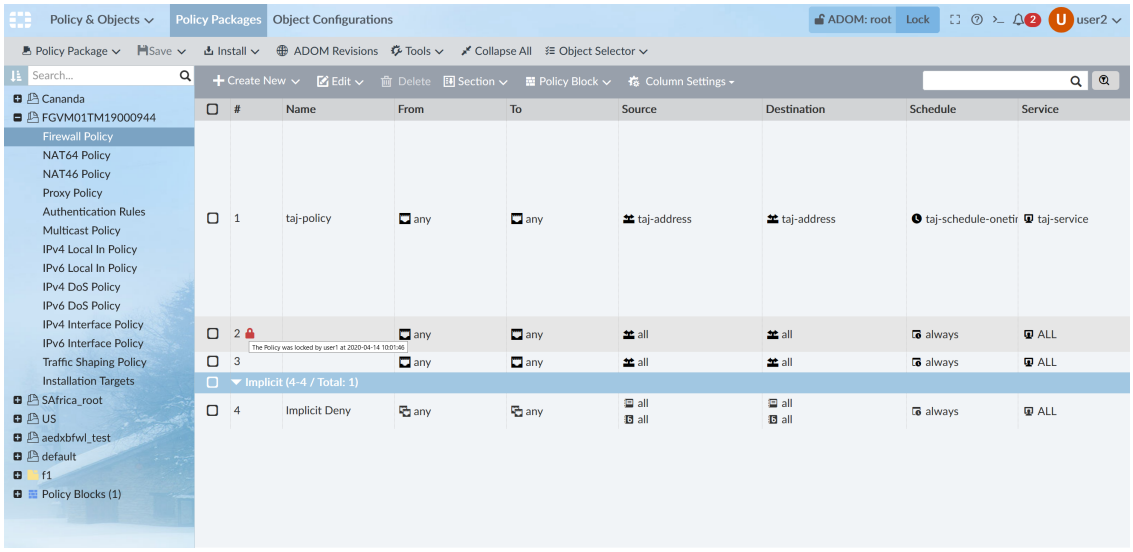
```
config system global
   set workspace-mode normal
   set per-policy-lock enable
end
```

To lock a policy:

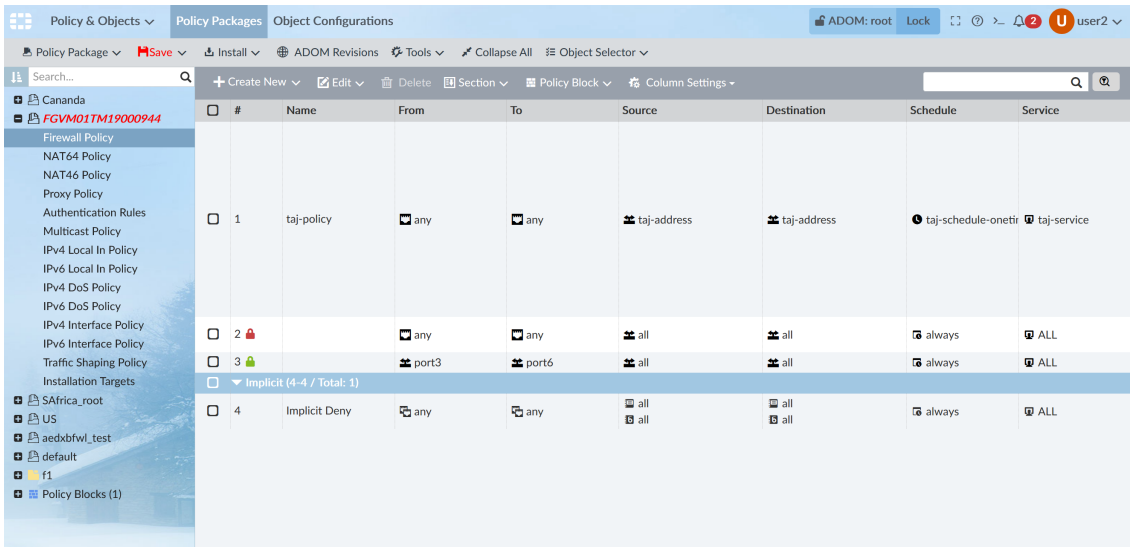
1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the policy package list, select the policy package, and right-click on the policy and select *Edit*.
   The *Edit IPv4 Policy* pane opens.
4. In the *Edit IPv4 Policy* pane, modify the policy and then click *OK*.
   A green padlock icon in the locked state is shown next to the policy name to indicate that it is locked by the current user.



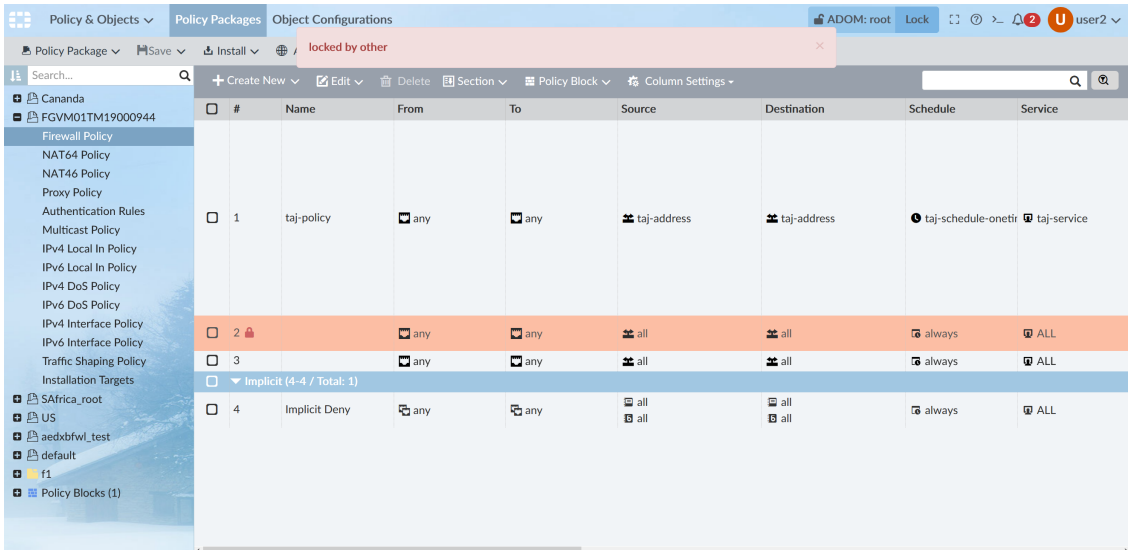
Others see a red padlock icon with details indicating that this policy was locked by some other user.



Once you lock a policy, other users cannot modify this policy, but they can still modify other unlocked policies.

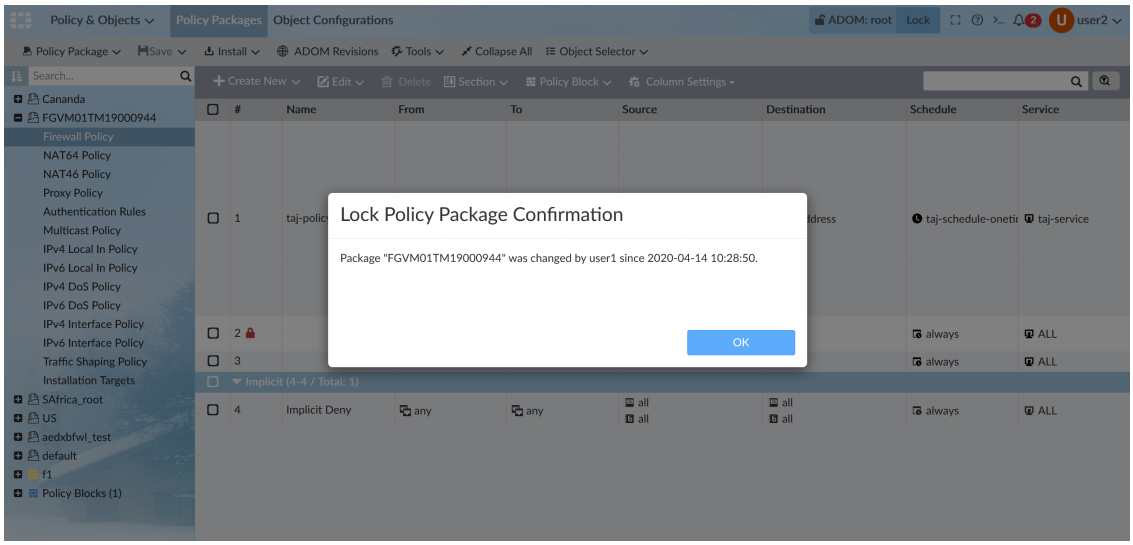


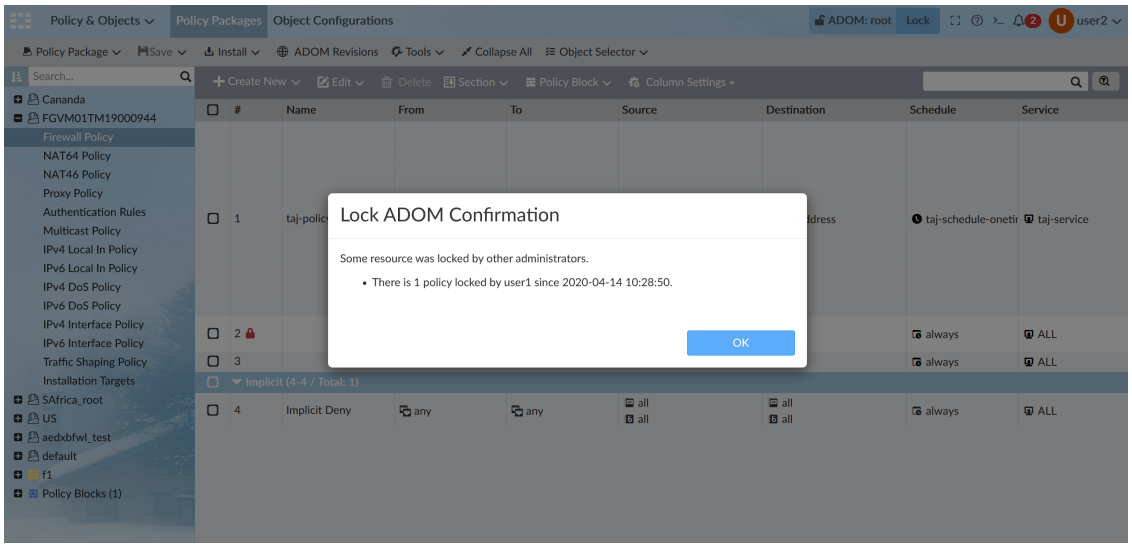
For instance, here, *user2* is unable to edit policy 2 as it was locked by the other user.



You can still lock the policy package or the whole ADOM with confirmation.

Other users are now unable to make changes to this policy package and cannot lock the ADOM.





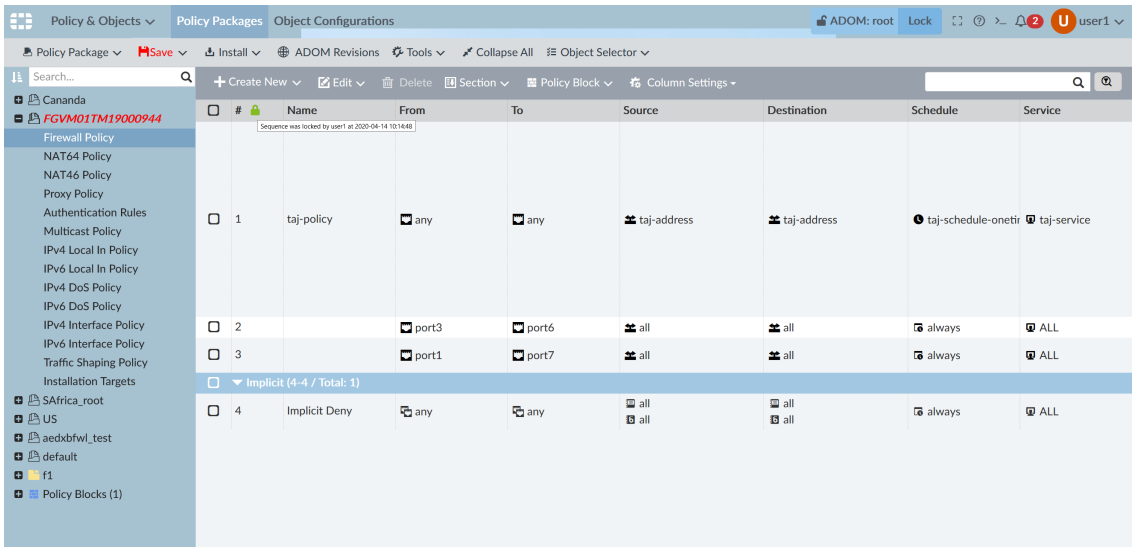
5. Click *Save* in the toolbar to save your changes.

Sequence lock:

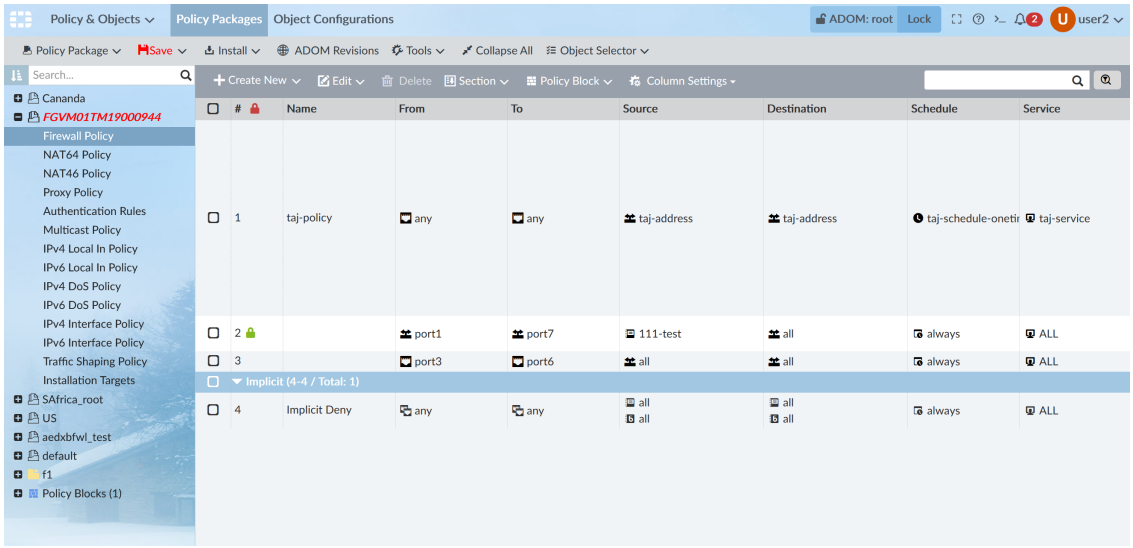
A policy sequence can be locked by creating, deleting, moving, cloning, or inserting policies.

The sequence lock ensures that the order of the policies is managed by one user at any given time.

If you set up a sequence lock, you see a green padlock icon at the top.



Other users see a red padlock icon at the top and cannot create, delete, clone, or insert policies, but they can still modify existing unlocked policies.



Once a sequence is locked, others are unable to lock the related policy package and ADOM.

Fabric Management Platform

This section lists the new features added to FortiManager for Fabric Management Platform. They are organized into the following sections:

Automation and connectors

This section lists the new features added to FortiManager for automation and connectors.

List of new features:

SDN connector to VMware vCenter

You can create SDN connectors for VMware vCentre to allow FortiGate to retrieve dynamic addresses from VMware vCenter via FortiManager.

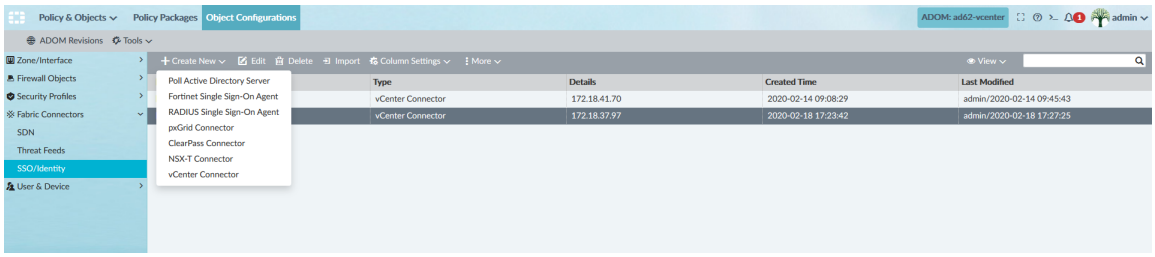
Following is an overview of how to configure an SDN connector for VMware vCenter:

1. Create an SDN connector for VMware vCenter. See Creating SDN connectors for VMware vCenter on page 41.
2. Create a dynamic address object that references the SDN connector for VMware vCenter. See Creating dynamic addresses on page 43.
3. Create a firewall policy. See Creating firewall policies on page 44.
4. Install the changes to FortiGate. See Installing changes to FortiGate on page 45.
   FortiGate can retrieve dynamic addresses from VMware vCenter via FortiManager.
   This example assumes that VMware vCenter is already set up.

Creating SDN connectors for VMware vCenter

To create SDN connectors for VMware vCenter:

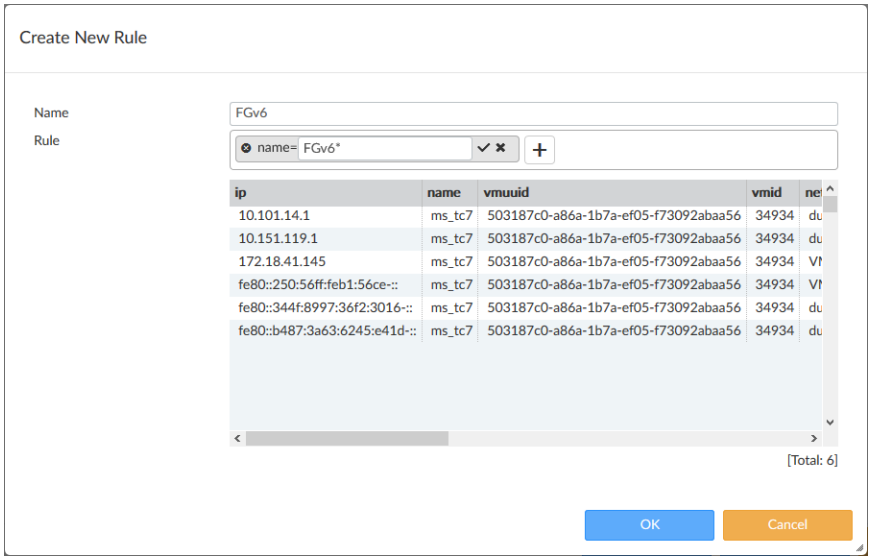
1. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *SSO/Identity*.
2. Click *Create New* > *vCenter Connector*.
   The pane opens.



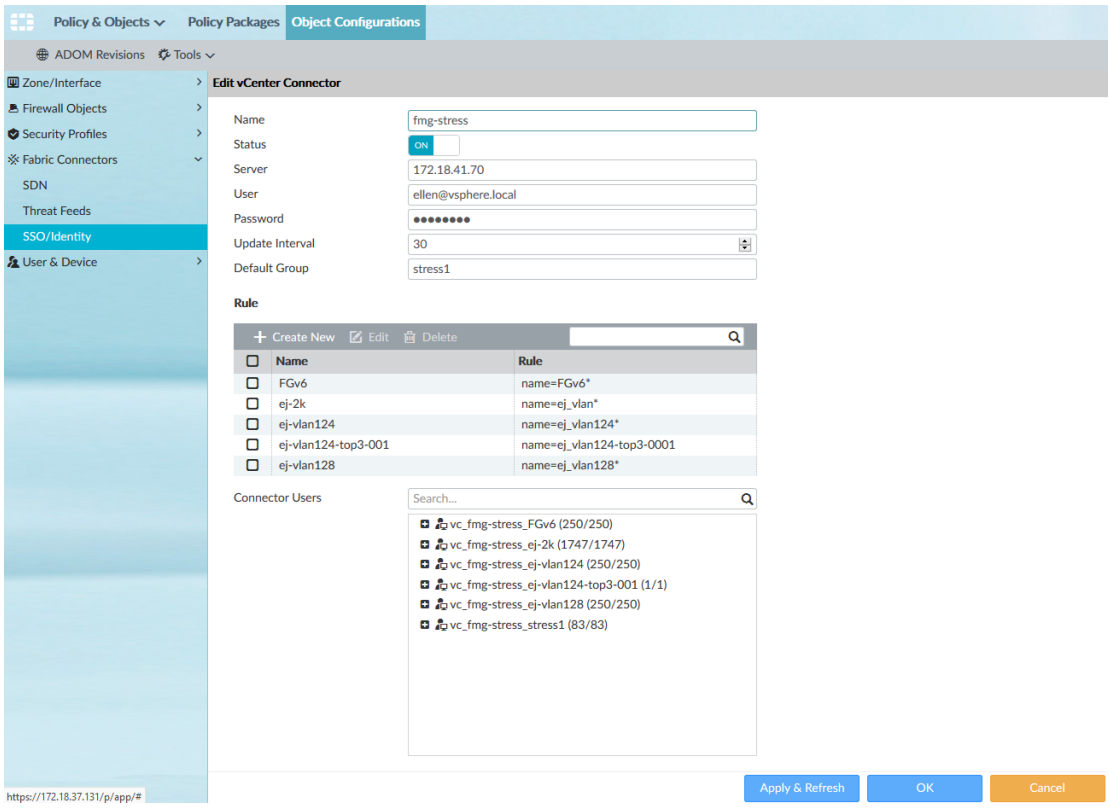
3. Complete the following options, and click *Apply & Refresh*:

The *Rule* section is displayed.

4. Under *Rule*, click *Create New*.
5. Complete the following options, and click *OK*.



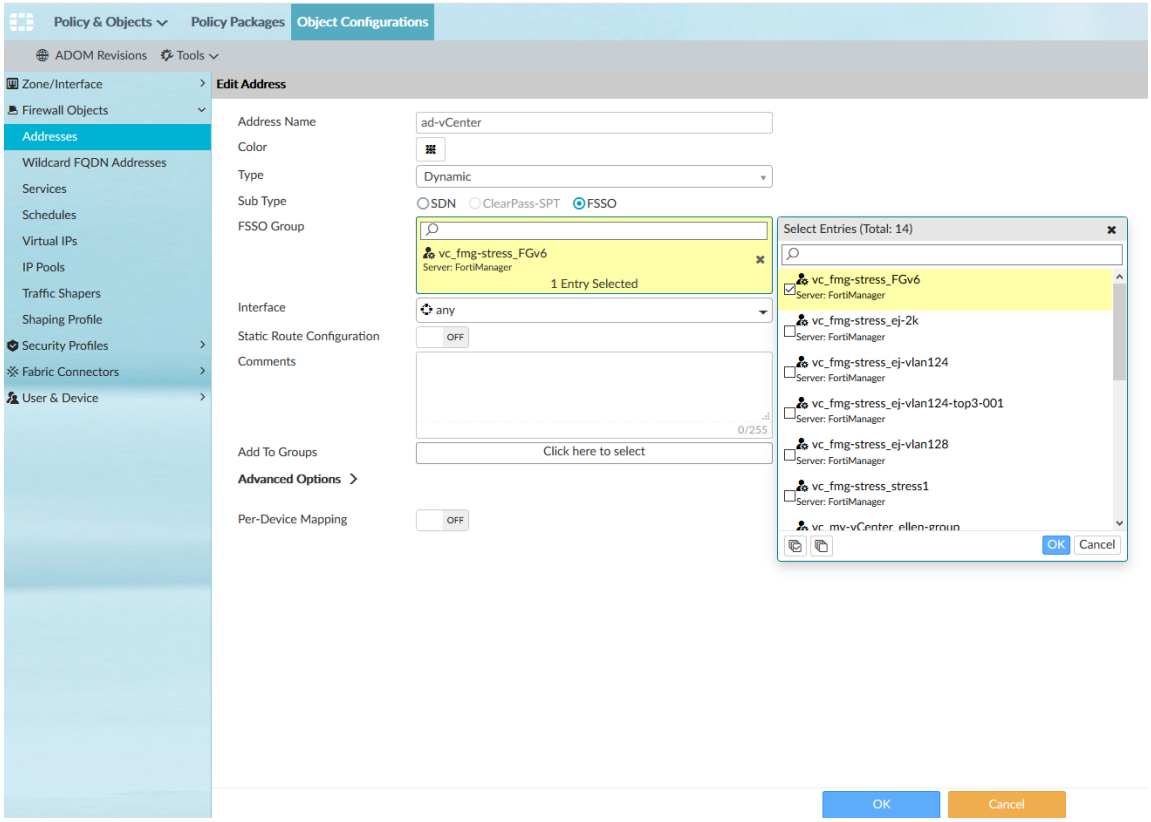
FortiManager retrieves IP addresses from the VMware vCenter server.



Creating dynamic addresses

To create dynamic addresses:

1. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Addresses*.
2. Click *Create New* > *Address*, or double-click an existing address object to open it for editing.
3. Complete the following options, and click *OK*.
   a. In the *Address Name* box, type a name.
   b. In the *Type* box, select *Dynamic*.
   c. Beside *Sub Type*, select *FSSO*.
   d. In the *FSSO Group* box, select the SDN connector that you created.
   e. Set the remaining objects as desired.



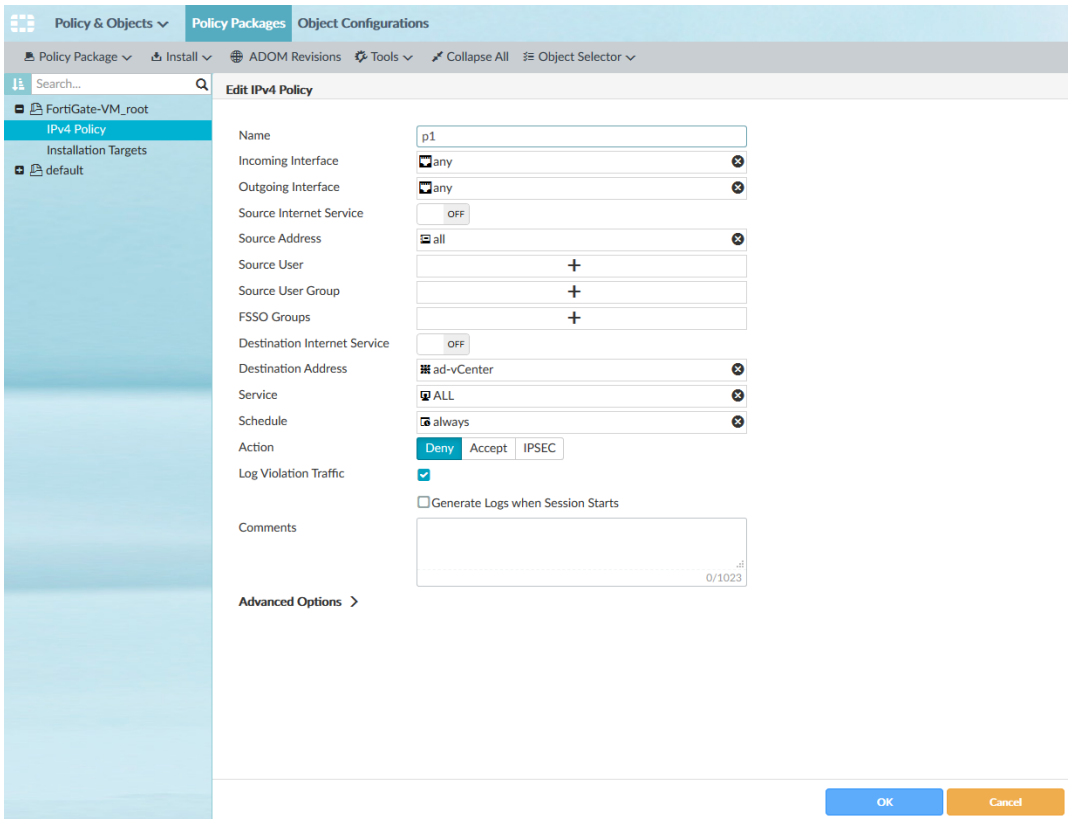
The dynamic address is created.

Creating firewall policies

To create firewall policies:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, click IPv4 Policy under the target FortiGate.

3. Click *Create New* , or double-click an existing policy to open it for editing.



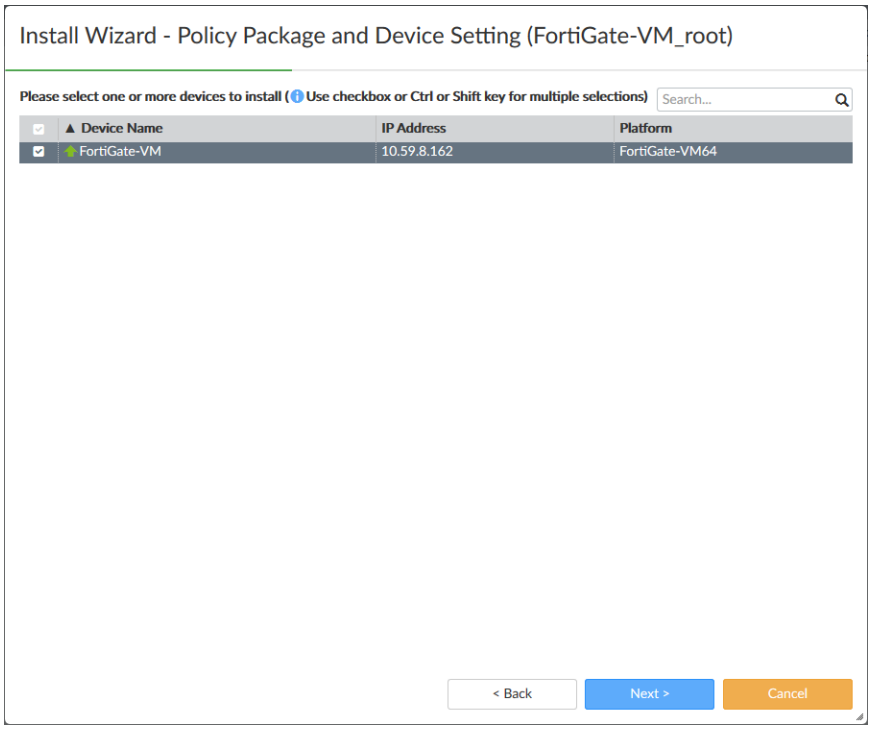
4. Complete the options, and click *OK*.
   The policy package is created.

Installing changes to FortiGate

To install changes to FortiGate:

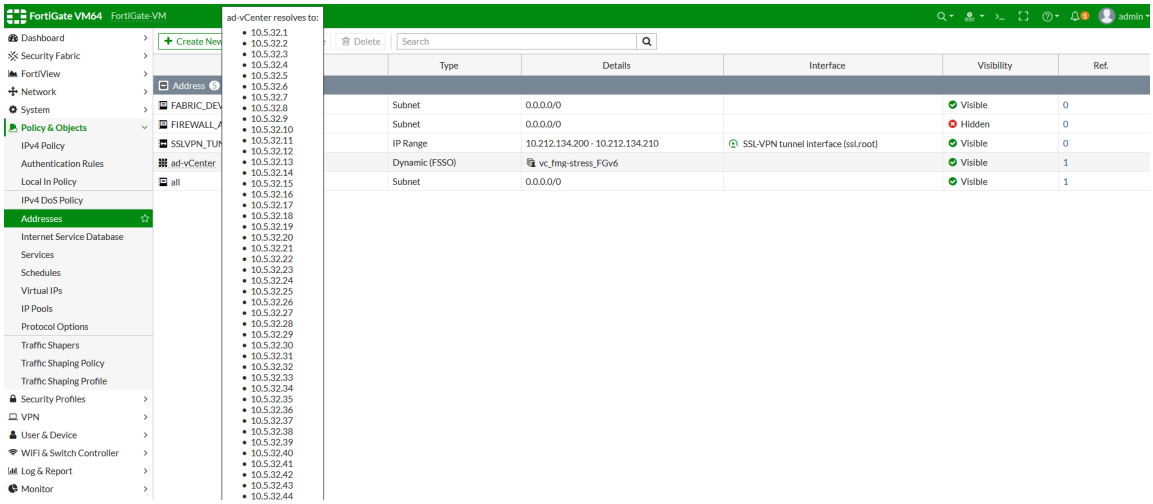
1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, right-click *Installation Targets* under the target FortiGate, and select *Install Wizard*.
   The *Install Wizard* dialog box opens.
3. Select *Install Policy Package & Device Settings*.

4. In the *Policy Package* list, select the policy package, and click *Next*.



5. Complete the options, and click *Next*.
   The policy package is installed.

   FortiGate can retrieve dynamic addresses from VMware vCenter via FortiManager.



Support multiple fabric connectors to Aruba ClearPass in the same ADOM

You can create multiple Aruba ClearPass connectors in each FortiManager ADOM, and then add them to a user group object, which you can install to FortiGates via a policy package. After the policy package is installed, FortiGate can use the multiple ClearPass connectors in the ADOM to connect to multiple CCPM (Configure ClearPass Policy Manager) servers.

Following is an overview of how to use multiple ClearPass connectors:

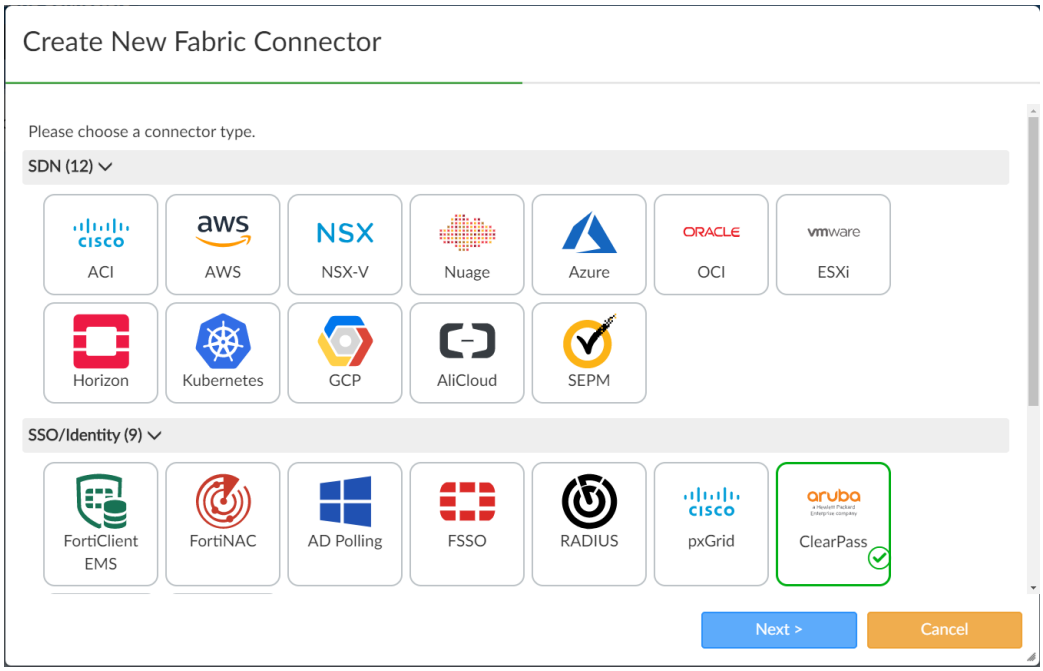
1. Create multiple ClearPass connectors in an ADOM. See Creating multiple ClearPass connectors in an ADOM on page 47.
2. Get roles and users from ClearPass. See Getting roles and users from ClearPass on page 48.
3. Create a user group object that references multiple ClearPass connectors. See Creating user groups on page 48.
4. Add the user group to a policy package, and install the policy package to FortiGate. See Installing policy packages to FortiGate on page 48.
   FortiGate uses the ClearPass connectors to connect to multiple CCPM servers.

This example assumes that Aruba ClearPass is already set up.

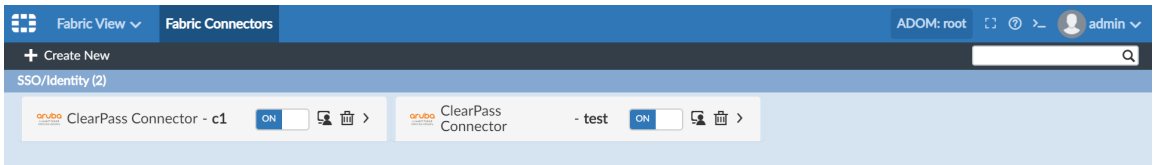
Creating multiple ClearPass connectors in an ADOM

To create multiple Aruba ClearPass connectors:

1. Ensure you are in the correct ADOM.
   This example uses the root ADOM.
2. Create a Clear Pass connector.
   a. Go to *Fabric View* > *Fabric Connectors*.
   b. Click *Create New* > *ClearPass*, and click *Next*.



   c. Complete the options, and click *OK*.
   The ClearPass connector is created.
3. Create another ClearPass connector.
   The multiple fabric connectors for Aruba ClearPass are displayed in the root ADOM.



Getting roles and users from ClearPass

To get roles and users from ClearPass:

1. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* >*SSO/Identity*.
2. Double-click a ClearPass connector to open it for editing, and click *Apply & Refresh*.
   FortiManager retrieves the roles and users from ClearPass.
3. Repeat this procedure for all ClearPass connectors in the ADOM.

Creating user groups

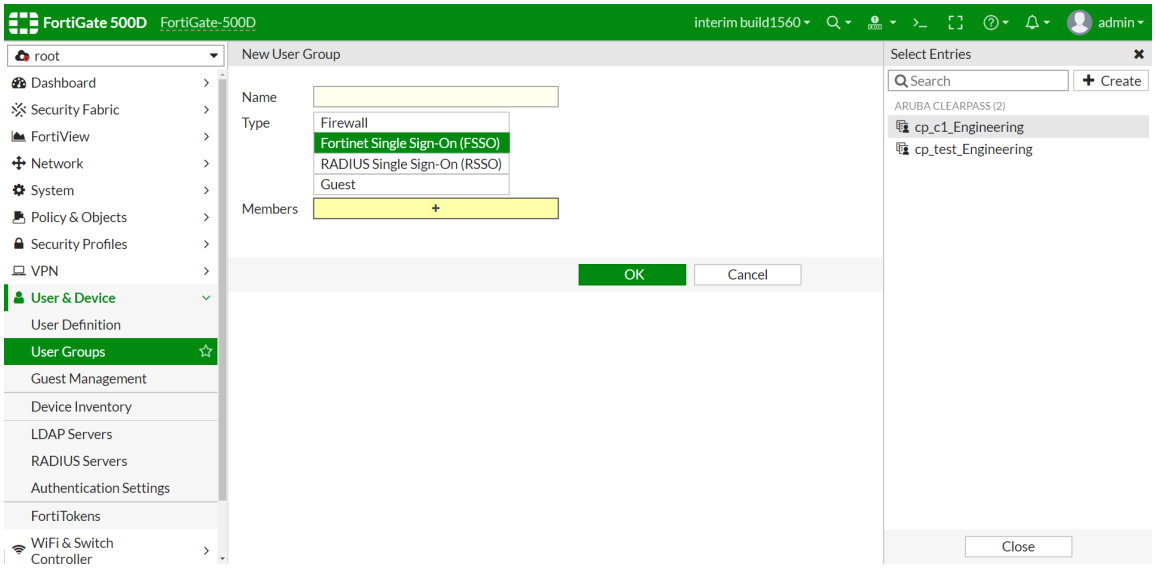
To create user groups:

1. Go to *Policy & Objects* > *Object Configurations* > *User & Device* > *User Groups*.
2. Click *Create New*.
3. In the *Group Name* box, type a name for the group.
4. Beside Type, select *FSSO/SSO Connectors*, and select the *Aruba ClearPass* connectors.
5. Set the remaining options, and click *OK*.

Installing policy packages to FortiGate

To install policy packages to FortiGate:

1. Go to *Policy & Objects* > *Policy Packages*.
2. Use the new user group in a policy package, and install the policy package to FortiGate.
   After the policy package is installed to FortiGate, FortiGate can use multiple CCPM servers. FortiGate distinguishes between multiple connectors by the user names contained in each ClearPass connector.



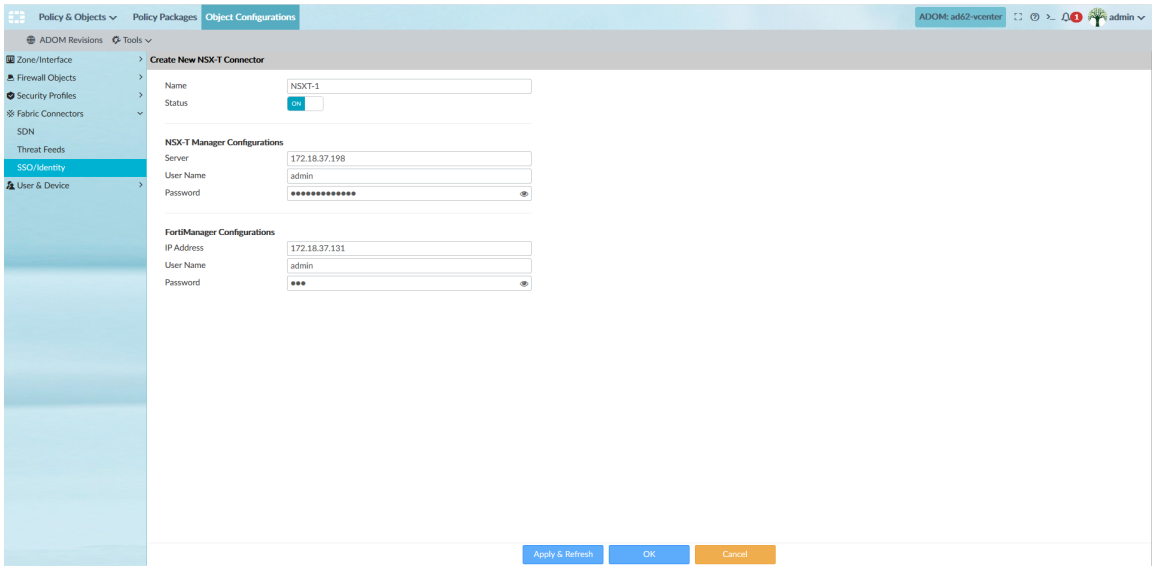
Support multiple VMware NSX-T connectors in the same ADOM

You can create multiple VMware NSX-T connectors in each FortiManager ADOM.

To create multiple VMware NSX-T connectors:

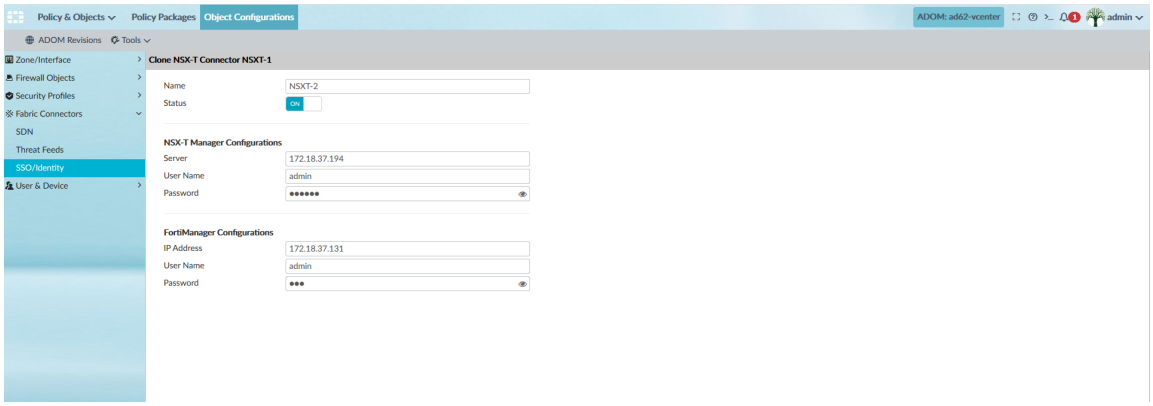
1. Ensure you are in the correct ADOM.
2. Create an NSX-T connector.
   a. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *SSO/Identity*.
   b. Click *Create New* > *NSX-T Connector*.
   c. Complete the options, and click *OK*.

   In the following example, a connector named *NSXT-1* is created.



3. Create another NSX-T connector.

   In the following example, a connector named *NSXT-2* is created.



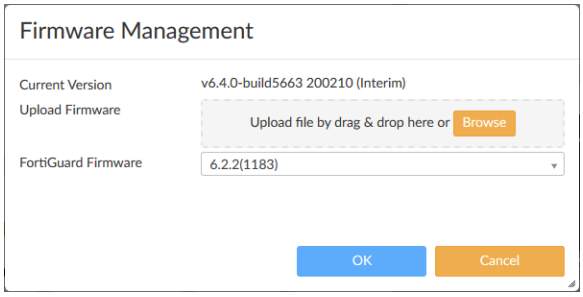
   The multiple fabric connectors for VMware NSX-T are displayed in the ADOM.

FortiManager firmware upgrade from FortiGuard servers

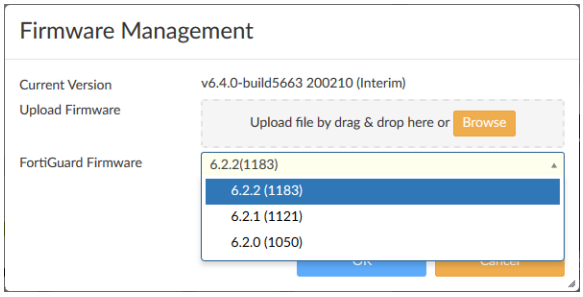
You can upgrade FortiManager firmware by using images available on FortiGuard servers. A green checkmark beside the available firmware images indicates the recommended FortiManager upgrade path. You can also upgrade to a firmware image that is not recommended if desired.

To upgrade FortiManager firmware in the GUI:

1. Go to *System Settings*.
2. In the *System Information* widget, beside *Firmware Version*, click *Update Firmware*.
   The *Firmware Management* dialog box opens.

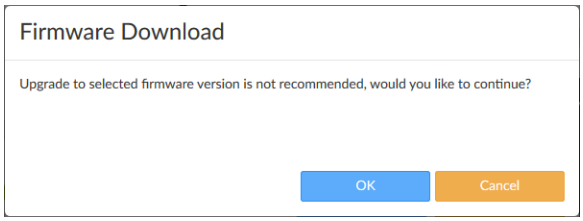


3. From the *FortiGuard Firmware* box, select the version of FortiManager for the upgrade, and click *OK*.
   The *FortiGuard Firmware* box displays all FortiManager firmware images available for upgrade. A green checkmark displays beside the recommended image for FortiManager upgrade.

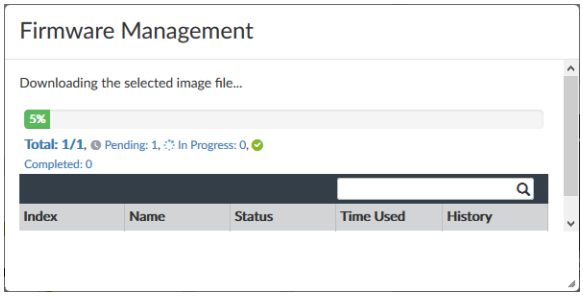


Because this image was captured before the release of FortiManager 6.4.0, a green checkmark is not yet available.

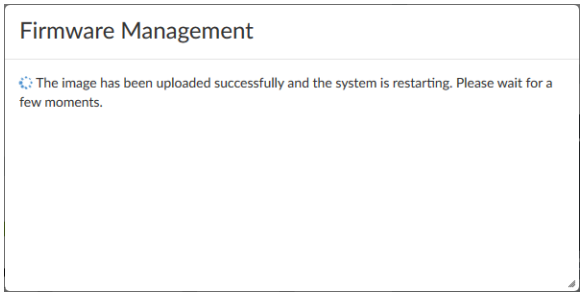
If you select an image without a green checkmark, a confirmation dialog box is displayed. Click *OK* to continue.



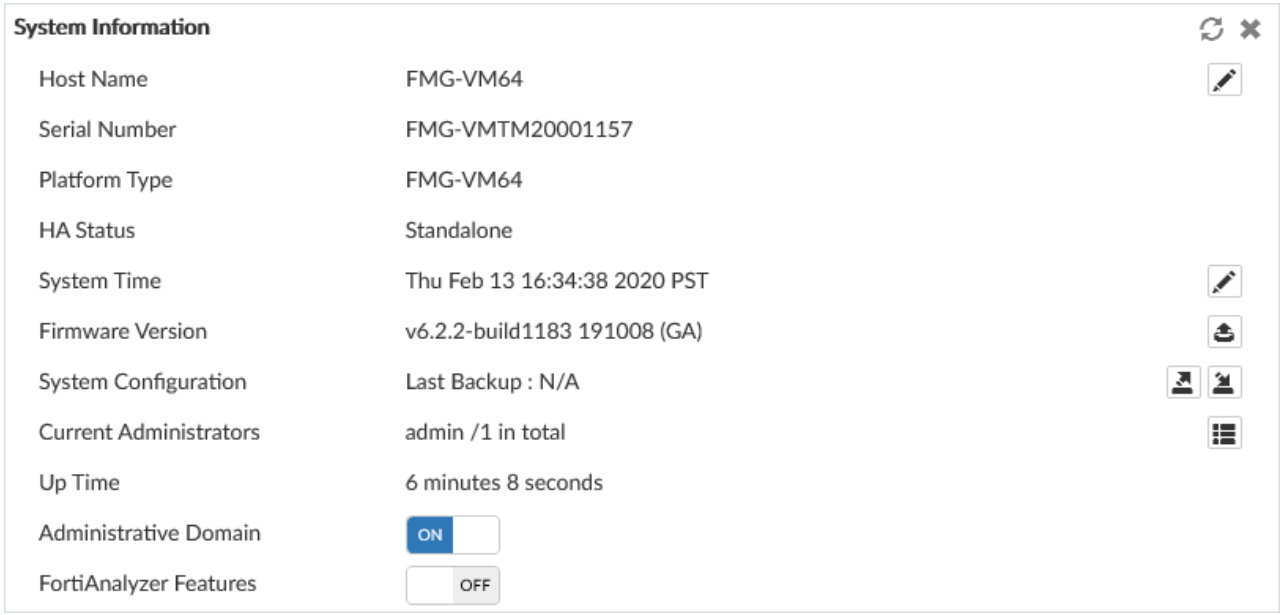
FortiManager downloads the firmware image from FortiGuard.



FortiManager uses the downloaded image to update its firmware, and then restarts.



After FortiManager restarts, the upgrade is complete.



SDN connector for Cisco ACI northbound API integration - 6.4.2

A new SDN connector type, *ACI-direct* has been added for Cisco ACI northbound API integration. It allows you to directly define dynamic firewall addresses for Cisco ACI.

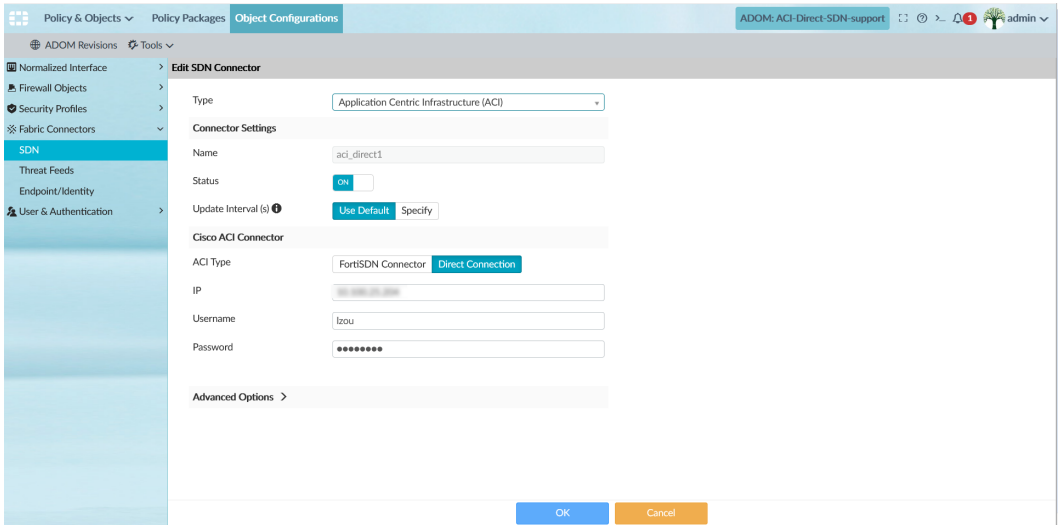
The following filters are supported:

- Tenant
- Application
- Endpoint group
- Tag

Fortinet SDN Connector is optional for this configuration.

To configure a Cisco ACI Direct connector:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Fabric Connectors* > *SDN*, and select the ACI SDN connector.
3. From the toolbar, select *Edit* to edit an existing SDN Connector.
   The *Edit SDN Connector* pane opens.

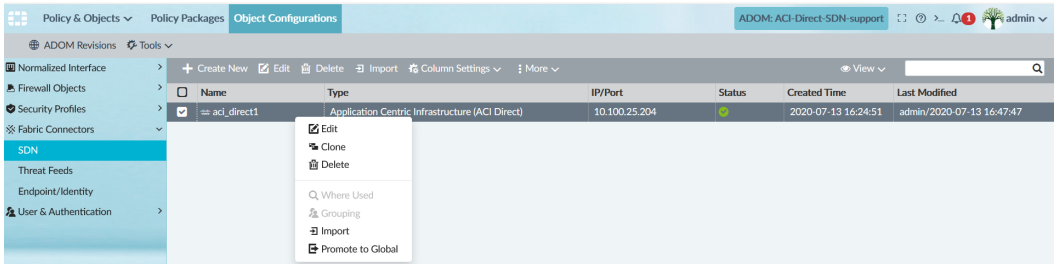


4. In the *Edit SDN Connector* pane, select *Direct Connection* as the *ACI Type*, and click *OK*.

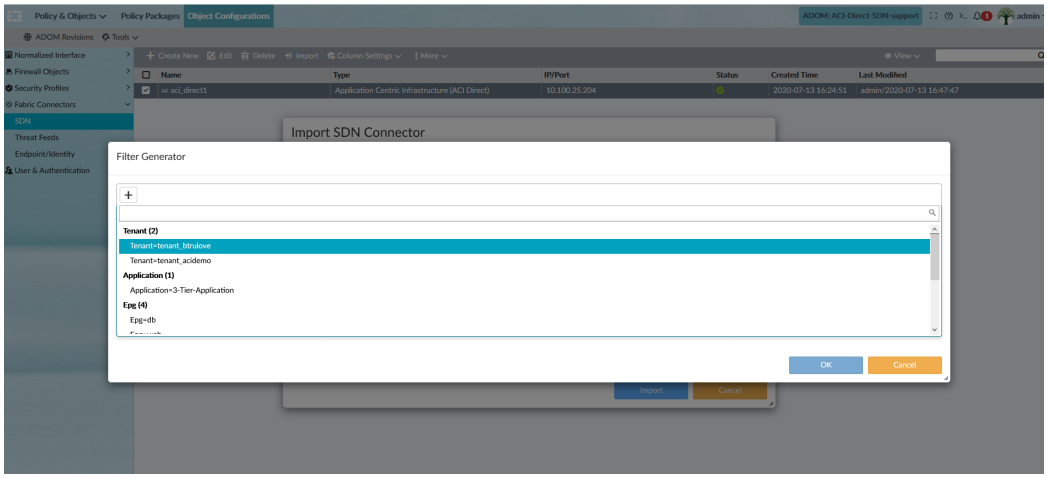
Alternatively, create a new SDN Connector by selecting *Create New* from the toolbar.

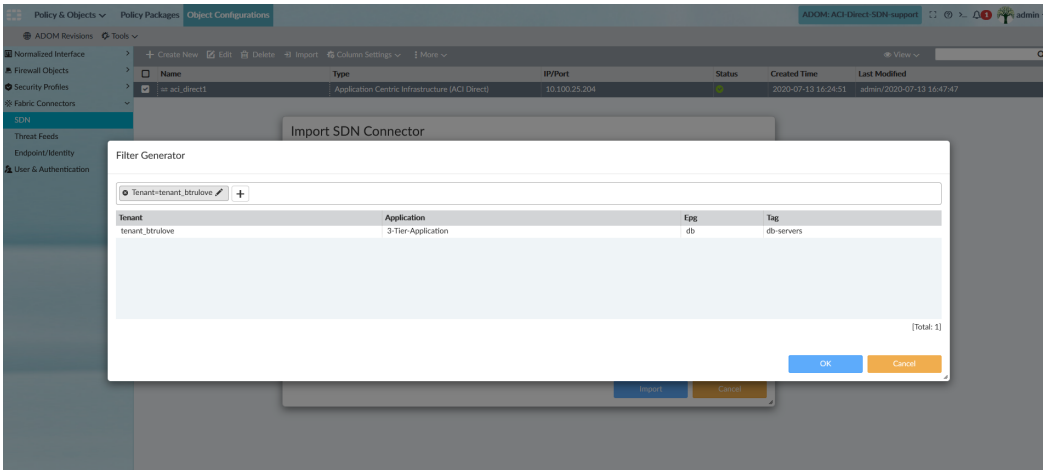
To import ACI objects from the Cisco ACI server:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Fabric Connectors* > *SDN*.
   The ACI-direct connector is displayed in the content pane.



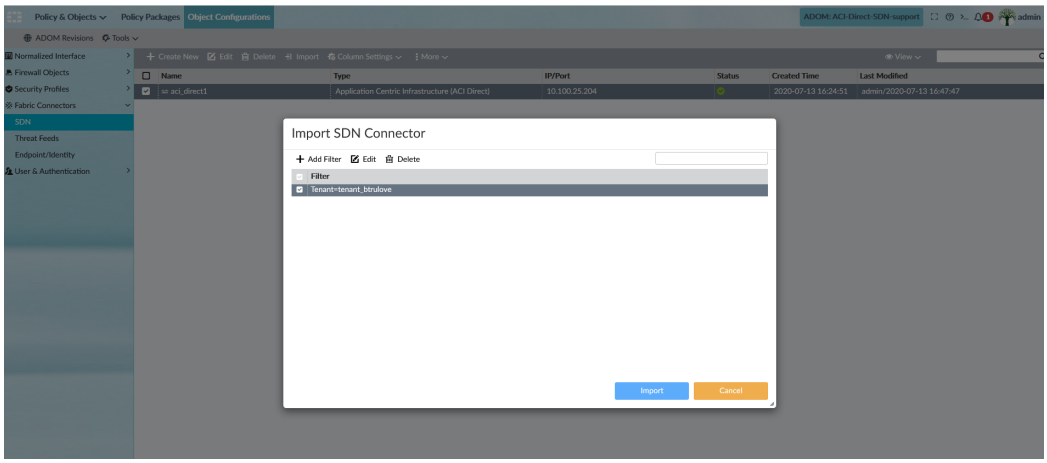
3. Right-click the ACI-direct SDN connector, here aci_direct1, and select *Import*.
   Once the processing bar in *Import SDN Connector* pane is filled, *Filter Generator* pane opens.
4. In the *Filter Generator* pane, select +, and add a filter from the list.



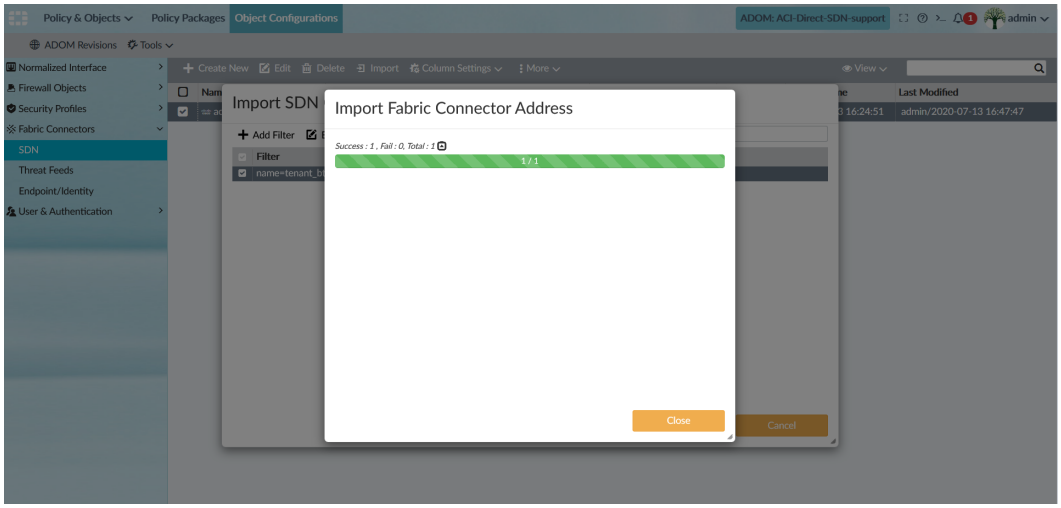


Click *OK*.
The *Import SDN Connector* pane opens.

5. Select the filter, and click *Import*.



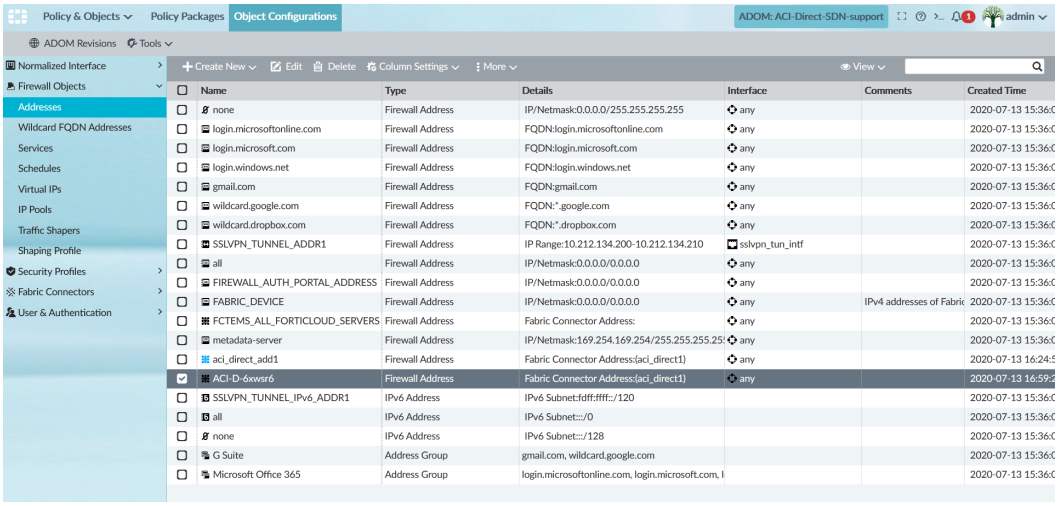
The fabric connector address is imported.



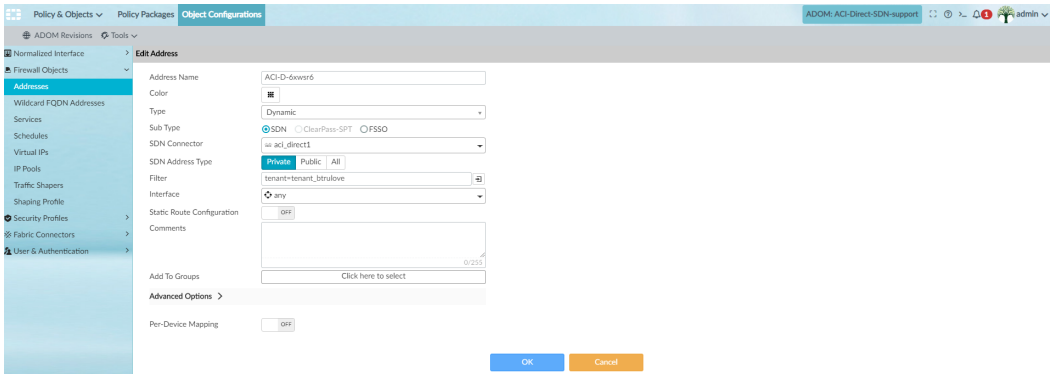
6. Click *Close*.
An ACI type dynamic address with the selected filter is automatically created.

To edit an ACI type dynamic address:

1. Go to *Policy & Objects* > *Object Configuration*, and in the tree menu under *Firewall Objects*, select *Addresses*.



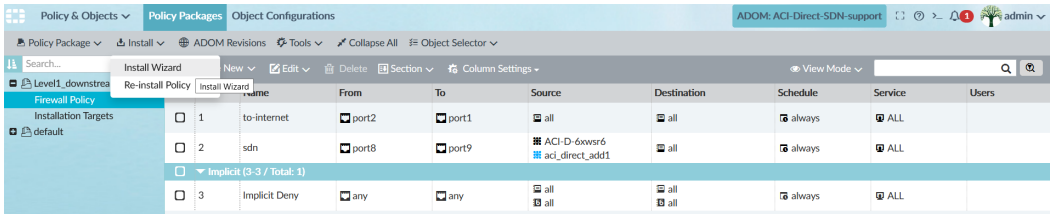
2. In the content pane, right-click the created address, and select *Edit*.
   The *Edit Address* pane opens.



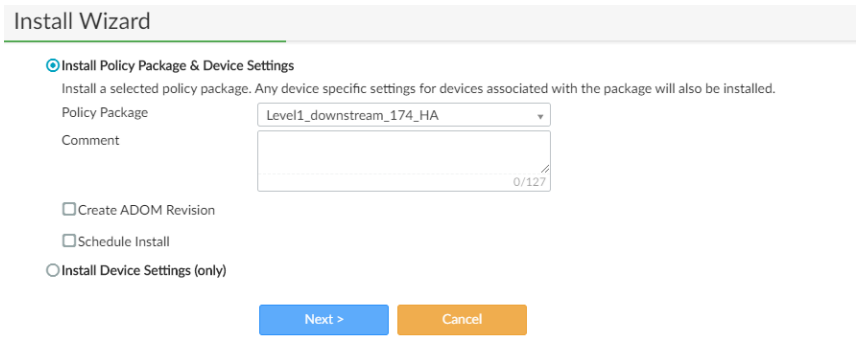
3. Configure the settings as needed, and click *OK*.

Using dynamic address in the policy:

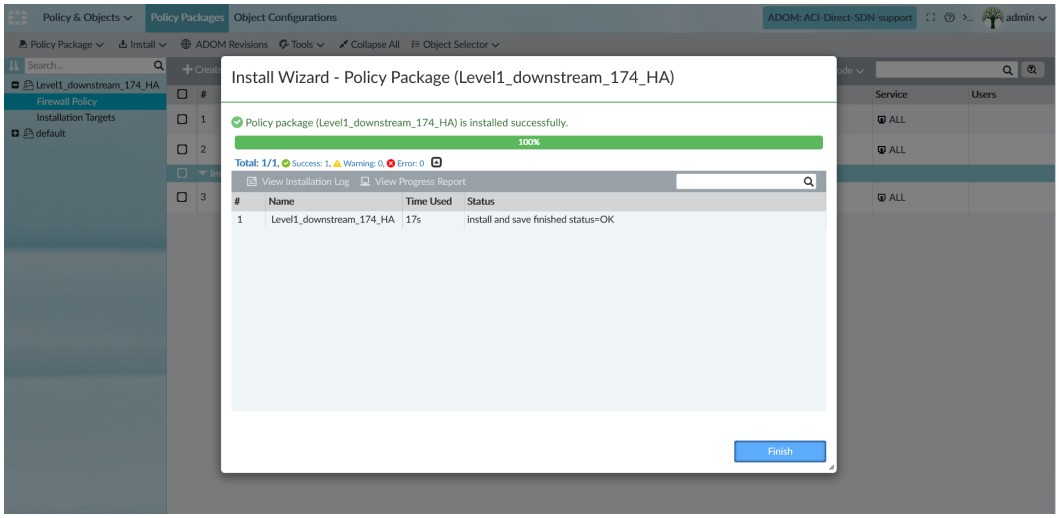
1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, select the package or the folder, here *Firewall Policy* under *Level1_downstream_174_HA*.



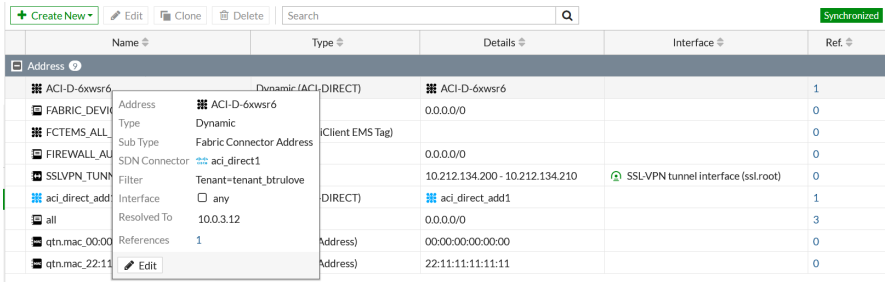
3. In the *Install* menu, select *Install Wizard*.
   The *Install Wizard* is displayed.



4. Select *Install Policy Package & Device Settings*, and click *Next*.
   The ACI direct type SDN address is successfully installed to the FortiGate.



5. Click *Finish*.
   You can verify if the installation was successful by going to *Policy & Objects* > *Addresses* in the FortiGate.



IMDSv2 support for FortiManager-VM on OCI - 6.4.4

FortiManager-VM on OCI uses Oracle Instance Metadata Service version 2 (IMDSv2) to query and retrieve metadata from OCI cloud. IMDSv2 provides enhanced security compared to version 1.

With IMDSv2:

- All requests to the IMDSv2 endpoints must include an authorization header. Requests that do not include the authorization header are rejected.

- Requests that are forwarded using the HTTP headers `Forwarded`, `X-Forwarded-For`, or `X-Forwarded-Host` are rejected.

To upgrade the instance metadata service on an OCI compute instance:

1. Verify that the instance uses an image that supports IMDSv2.
2. Identify and migrate requests to the legacy IMDSv1 endpoints to support IMDSv2 endpoints.
3. Disable all requests to the legacy IMDSv1 endpoints.

Single pane

This section lists the new features added to FortiManager for single pane.

List of new features:

Prompt admin to register FortiManager with FortiCloud

FortiManager VM users are now required to register their VM license or get a free trial license. You can register a hardware device directly from the *System Settings* > *Dashboard* pane with FortiCloud.

This topic contains the following section:

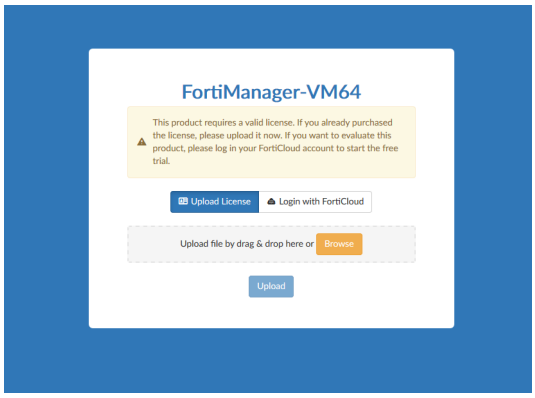
Registering a VM license

To download a VM license file, log in to FortiCloud, and click *Asset* > *Manage/View Products*. Select a device from the list, and click the link in the *License File* field.

To register a VM license:

1. Go to the FortiManager VM login page.
2. Click *Upload License*, and take one of the following actions:
   - Drag and drop the license file onto the field.
   - Click *Browse* to navigate to the location of your license file on your computer.

3. Click *Upload*.

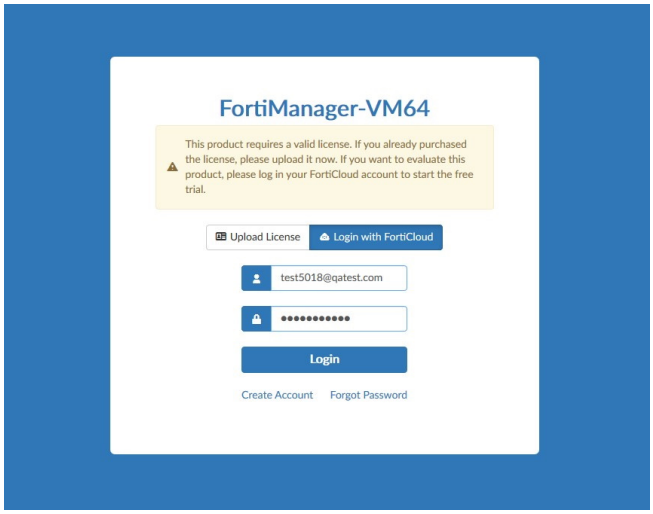


Getting a trial VM license

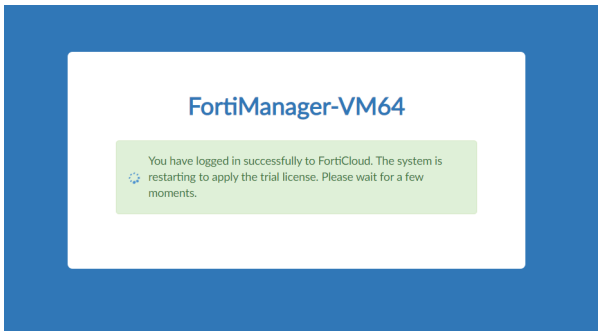
If a VM license is not associated with your FortiCloud account, you can get a free trial license for up to three devices. Trial licenses do not expire.

To get a trial VM license:

1. Go to the FortiManager VM login page.
2. Click *Login with FortiCloud*.
3. Enter your FortiCloud account credentials, and click *Login*. If you do not have a FortiCloud account, click *Create Account*.

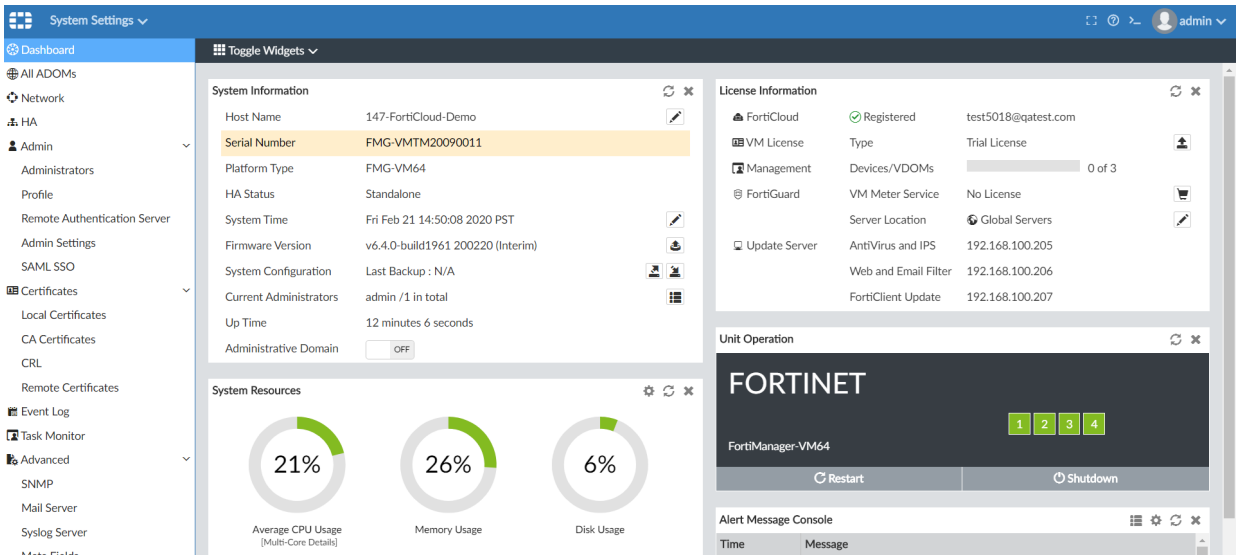


FortiManager VM connects to FortiCloud to get the trial license, and the system reboots.

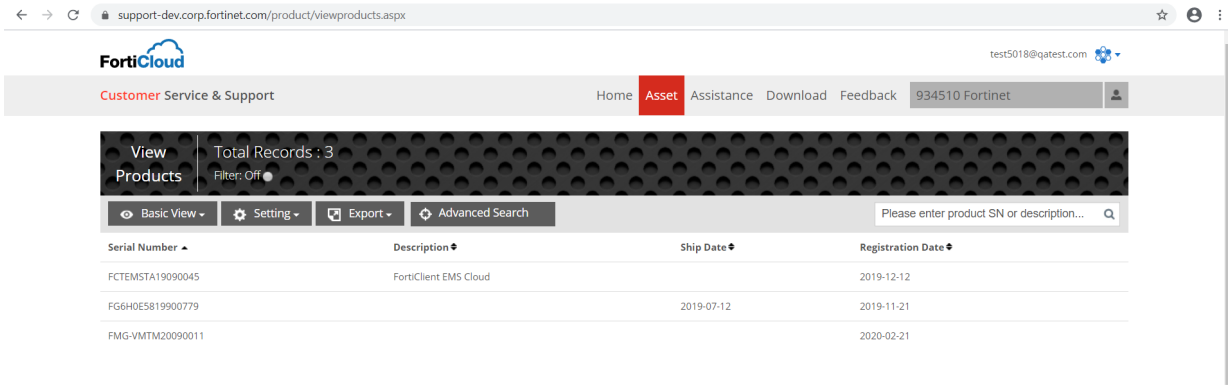


4. Log back into FortiManager VM.

5. Go to *System Settings* > *Dashboard* to view the license status in the in the *License Information* widget.



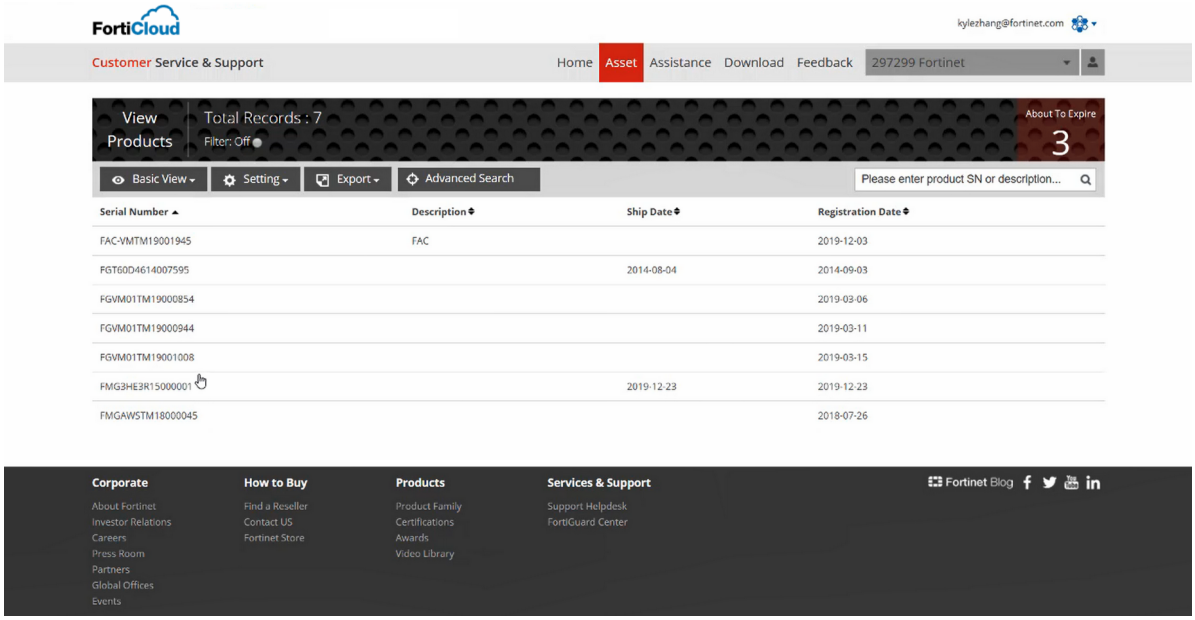
6. To view your trial license in FortiCloud, log in to your account, and click *Asset* > *Manage/View Products*.



Registering a hardware device

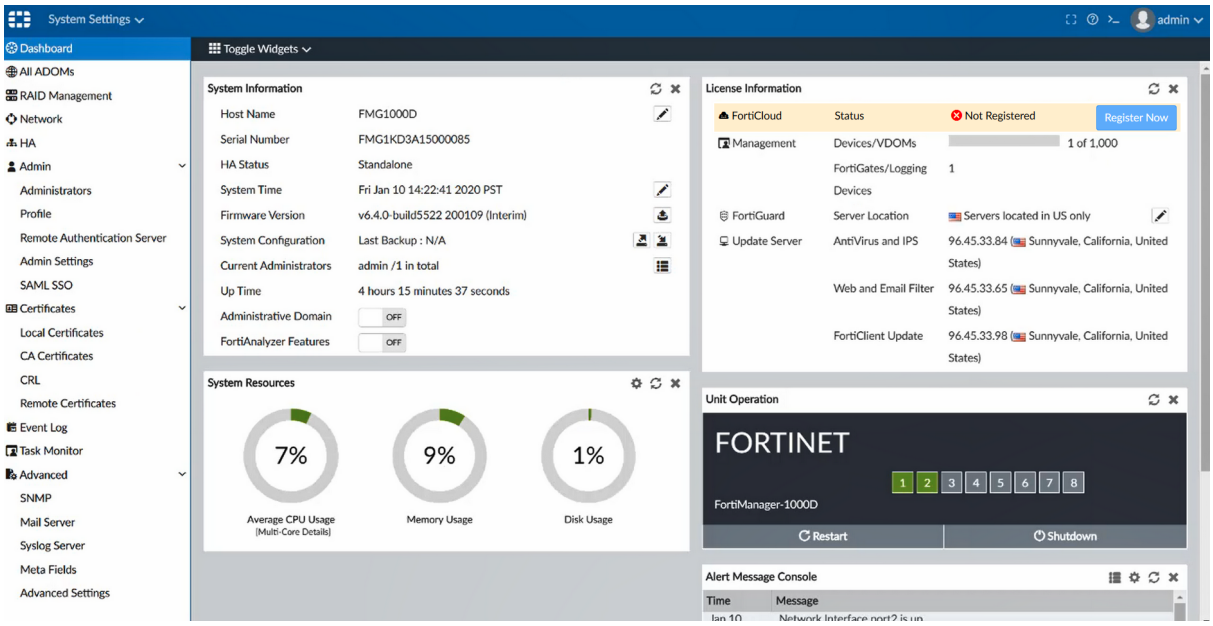
To register a hardware device:

1. To verify the license is not registered, log in to FortiCloud, and click the *Assets* tab. If you do not see your device, then it is not registered.

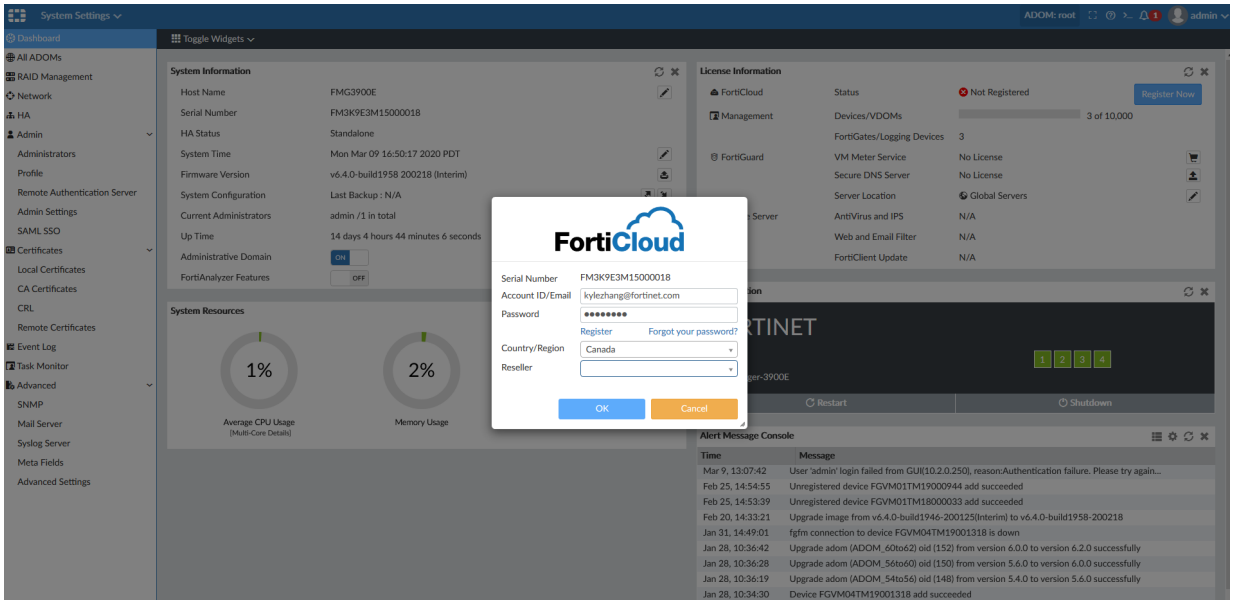


2. In FortiManager, go to *System Settings* > *Dashboard*.

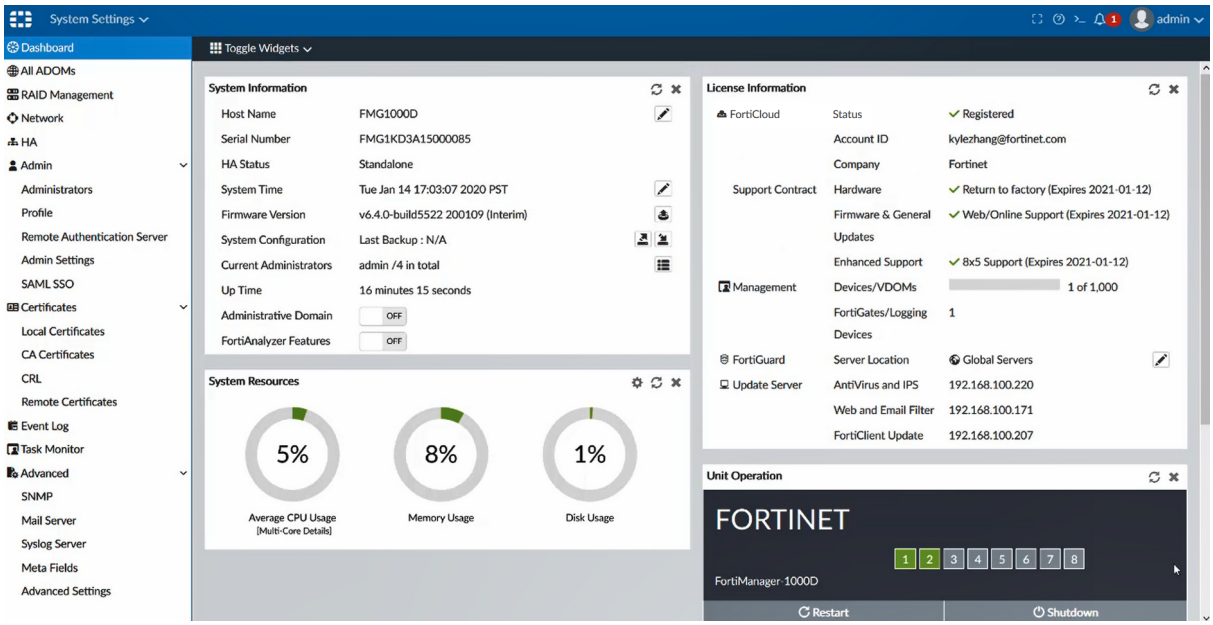
3. In the *License Information* widget, click *Register Now*.



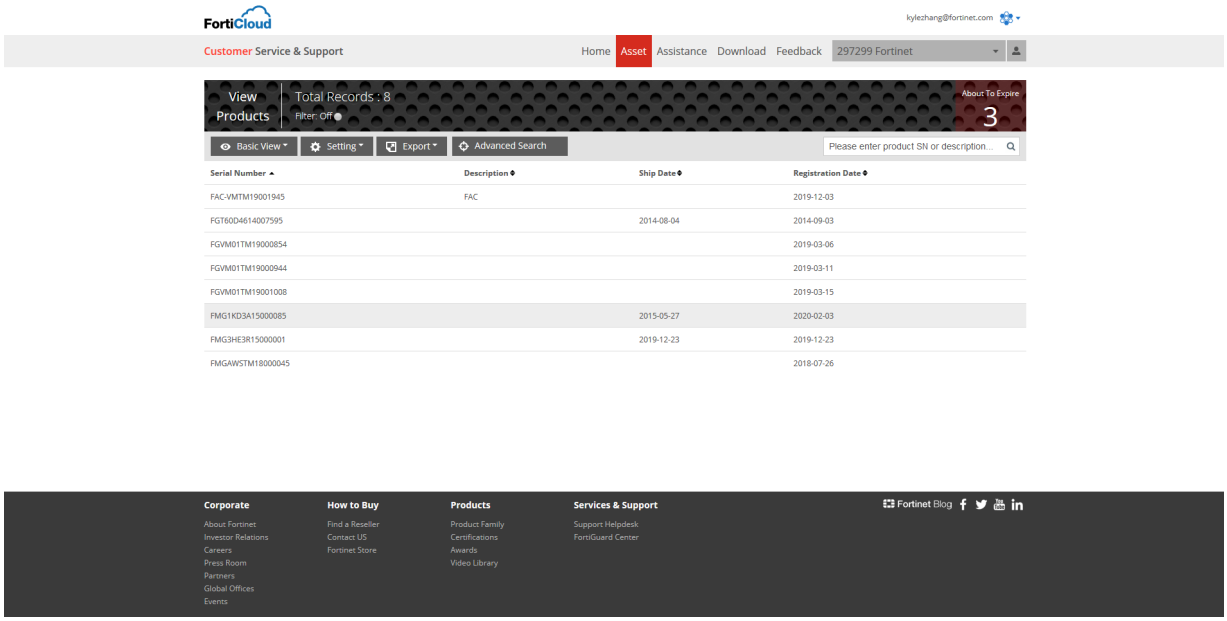
4. Enter your device information in the FortiCloud window, and click *OK*. FortiManager sends the information to FortiCloud.



After the information is synchronized, the *Status* changes to *Registered*.



5. Go back to the *Assets* page in FortiCloud to verify the device is registered.



Viewing license information with the CLI

You can view the license status and information by using the CLI.

To view the license status in the CLI:

```
get system status
```

To view the license information in the CLI:

```
diagnose debug vminfo
```

To connect the VM to FortiCloud when you set up the device:

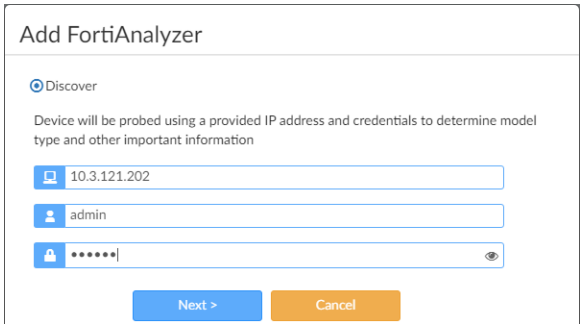
```
diagnose debug enable
diagnose debug application vmd <integer>
```

FortiManager support for FortiAnalyzer HA

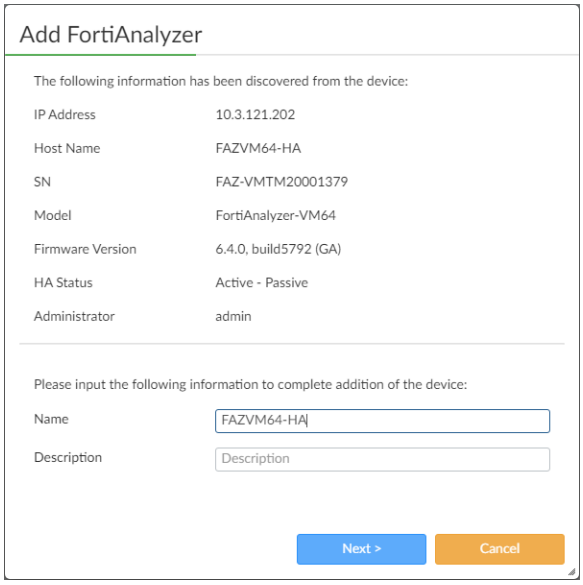
You can manage FortiAnalyzer HA via FortiManager. FortiManager retrieves the cluster member list and updates the information whenever it changes, including FortiAnalyzer HA failover or a change in members.

To enable support for FortiAnalyzer HA:

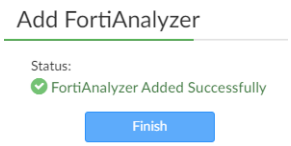
1. Go to *Device Manager* > *Device and Groups*.
2. Click the down arrow next to *Add Devices*. Select *Add FortiAnalyzer*.
   The *Add FortiAnalyzer* dialog opens.



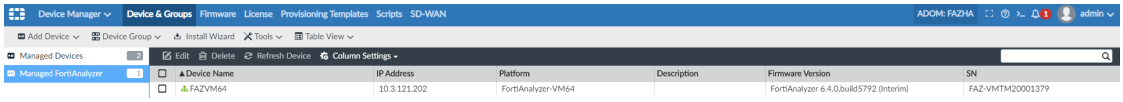
3. From the *Add FortiAnalyzer* box, add FortiAnalyzer HA to FortiManager DVM by HA cluster's VIP, and click *Next*.
   The FortiAnalyzer HA is discovered with its HA status information. Click *Next* to continue.



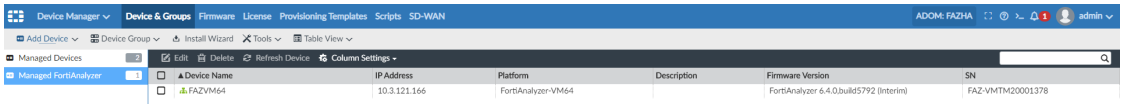
   FortiAnalyzer HA is added successfully. Click *Finish*.



4. In the tree menu, select *Managed FortiAnalyzer*. The device status icon is shown as the HA cluster and the SN is shown as the primary SN.



FortiManager DVM gets an update after the failover on FortiAnalyzer in 300 seconds. Here, the previous primary "FAZ-VMTM20001379" becomes the secondary, and the new primary is "FAZ-VMTM20001378".



You can get the HA status update immediately, select the FortiAnalyzer device and either click *Refresh Device* from the toolbar, or right-click and select *Refresh*.

To check the DVM device list in the CLI:

1. View the DVM device list once FortiAnalyzer HA is added to FortiManager:
   ```
   diagnose dvm device list
   ```
   It will have correct HA cluster information, including member list and role.
2. View the DVM device list after the failover on FortiAnalyzer:
   ```
   diagnose dvm device list
   ```
   It will have the updated HA cluster information. The previous primary changes to secondary and vice versa.

Enable management extensions in FortiManager

You can enable the following applications as part of management extensions in FortiManager:

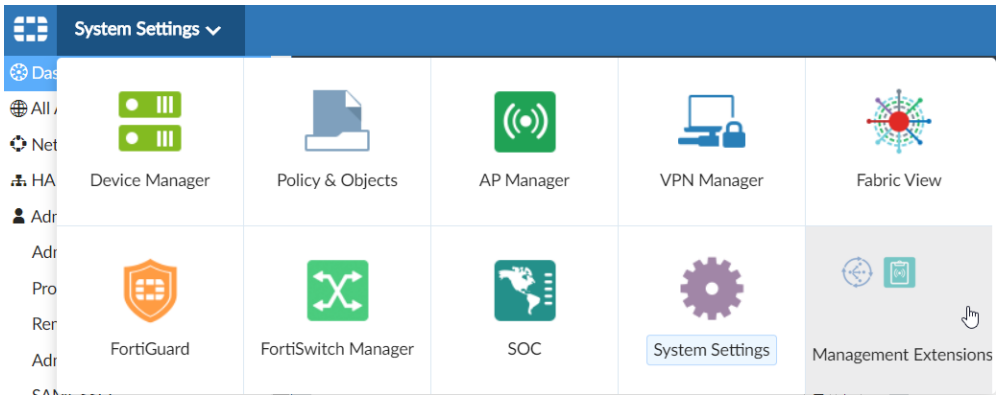
- SD-WAN Orchestrator
- Wireless Manager

When enabled, the management extension application is installed on FortiManager for you to use with FortiManager. You can enable management extension applications by using the GUI or CLI.

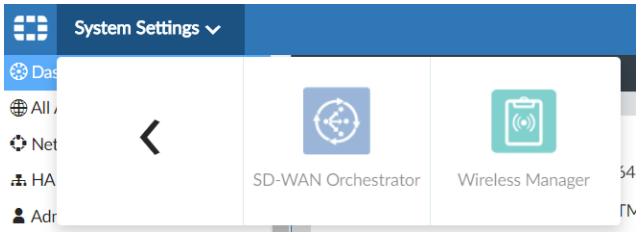
This feature uses Fortinet public DNS servers located at 208.91.112.52 or 208.91.112.53. By default, FortiManager is set to use these DNS server locations. You can check the location by going to *System Settings* > *Network*.

To enable management extension applications with the GUI:

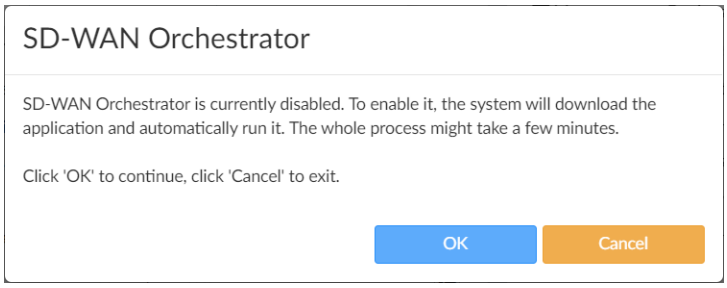
1. Go to *Management Extensions*.



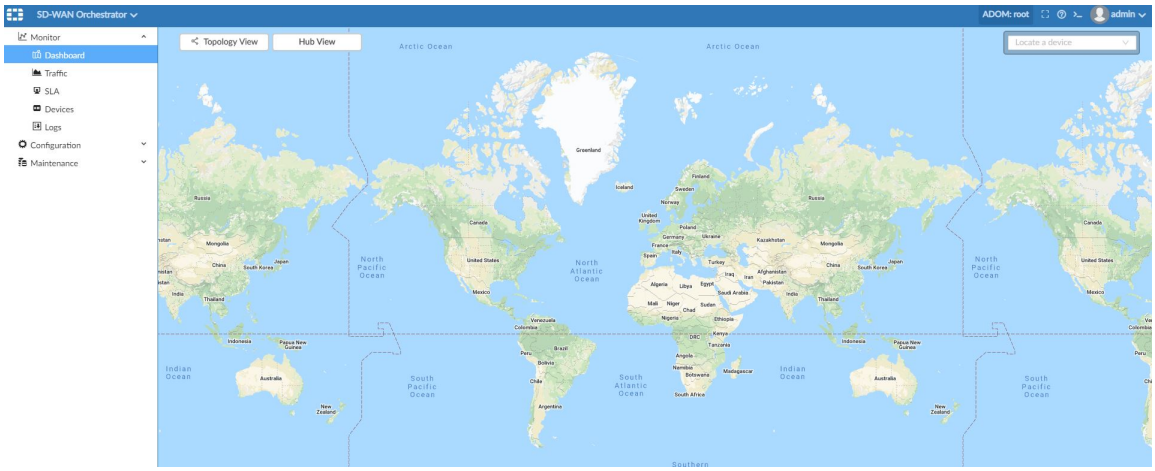
2. Click a management extension to enable it.
For example, click *SD-WAN Orchestrator*.



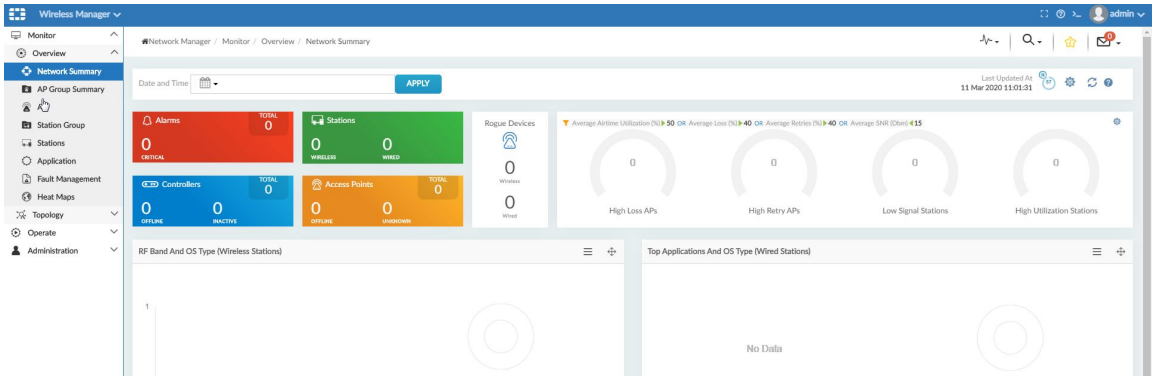
A confirmation dialog box is displayed.



3. Click *OK* to continue.
The management extension application is installed and opens. For example, SD-WAN Orchestrator opens.



Following is an example of the Wireless Manager application after being enabled:



To enable management extension applications with the CLI:

1. Enable the production registry:
```
FMG-VM64 # config system docker
(docker)# set status
enable  Enable production registry.
```
2. Enable the management application.
```
(docker)# set
fortiwlm  Enable/disable container.
sdwancontroller  Enable/disable container.
```

Licenses for management extension applications

FortiManager supports the following applications as part of management extensions:

- SD-WAN Orchestrator
- Wireless Manager

You can install the applications from the *Management Extensions* module in FortiManager. See Enable management extensions in FortiManager on page 65.

SD-WAN Orchestrator is free to install and is available with a valid support contract for FortiManager. However SD-WAN Orchestrator only supports managed FortiGates with an SD-WAN Orchestrator entitlement. The 360 Bundle contract for FortiGates includes the SD-WAN Orchestrator entitlement. The SD-WAN Orchestrator entitlement can also be purchased separately.

Wireless Manager is free to install and is available with a valid support contract for FortiManager. The support contract includes an *FWLM-BASE* license that lets you add up to three FortiAPs to Wireless Manager. A valid Wireless Manager license is required to add more than three FortiAPs to Wireless Manager.

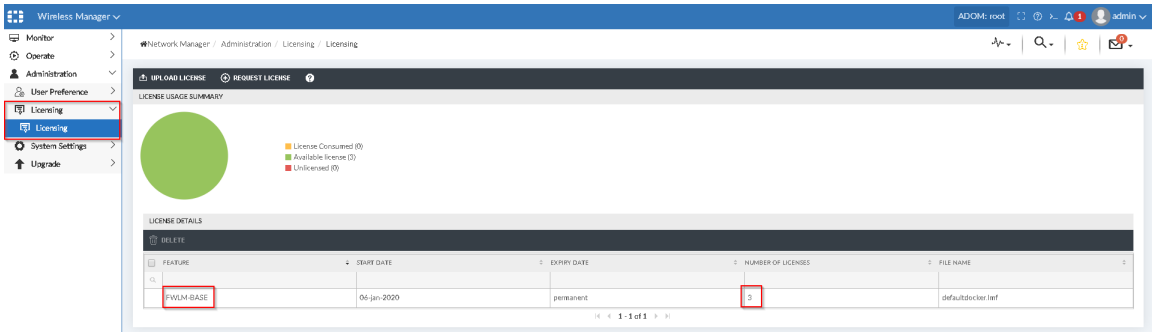
This topic contains the following sections about Wireless Manager:

Viewing license information

After you install the Wireless Manager application, you can view license information. This example shows how to view the FWLM-BASE license in Wireless Manager.

To view license information in Wireless Manager:

1. In Wireless Manager, go to *Administration* > *Licensing* > *Licensing*.
   The license details are displayed.



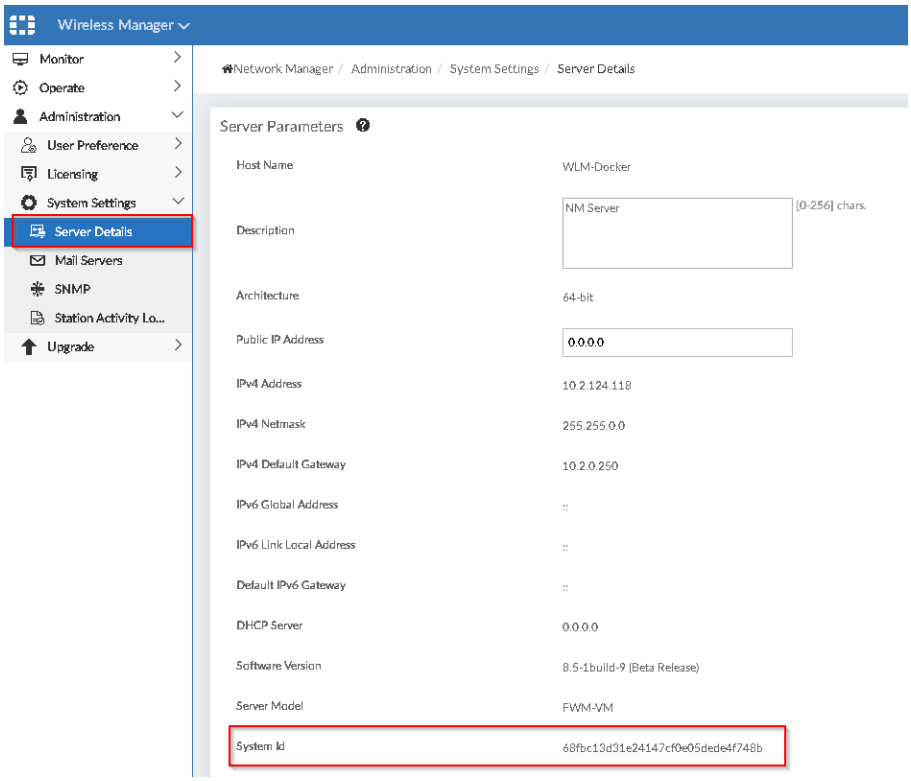
Obtaining the system ID for a license

When requesting a license for *Wireless Network Manager Evaluation License Certificate*, you must add the provided registration code to the account on the Customer Service and Support site (https://support.fortinet.com) and the system ID for Wireless Manager. You can obtain the system ID from Wireless Manager.

To obtain the system ID for Wireless Manager:

1. In Wireless Manager, go to Administration > System Settings > Server Details.
   The *Server Parameters* are displayed.

2. Scroll down to the *System ID* option.

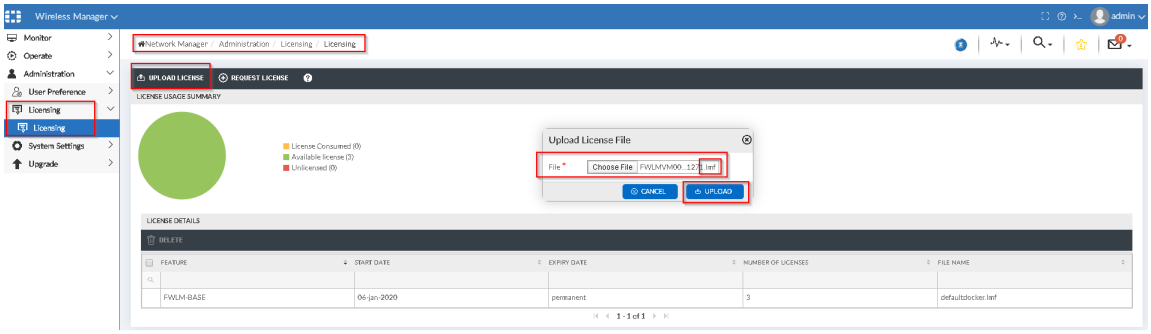


Uploading a license

After downloading the license file from the Customer Service and Support site, you can upload the license to Wireless Manager.

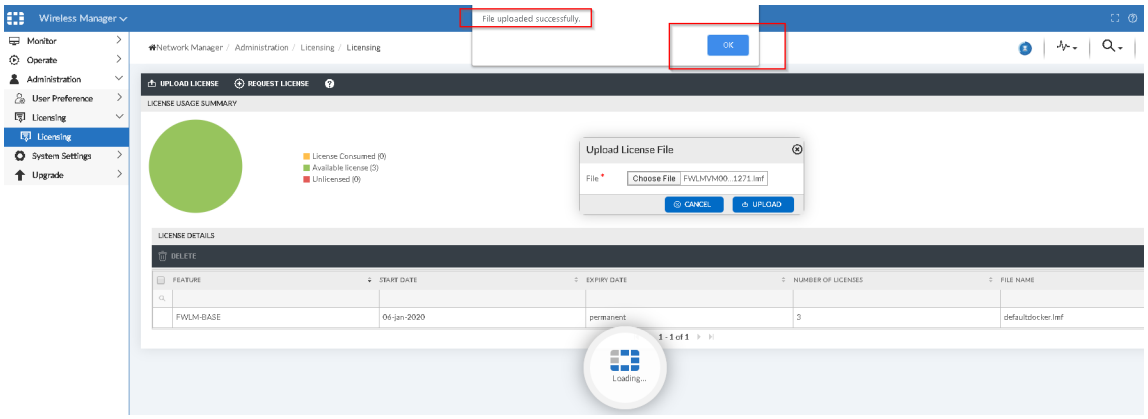
To upload a license to Wireless Manager:

1. In Wireless Manager, go to *Administration* > *Licensing* > *Licensing*.
2. Click *Upload License*.
   The Upload License dialog box is displayed.

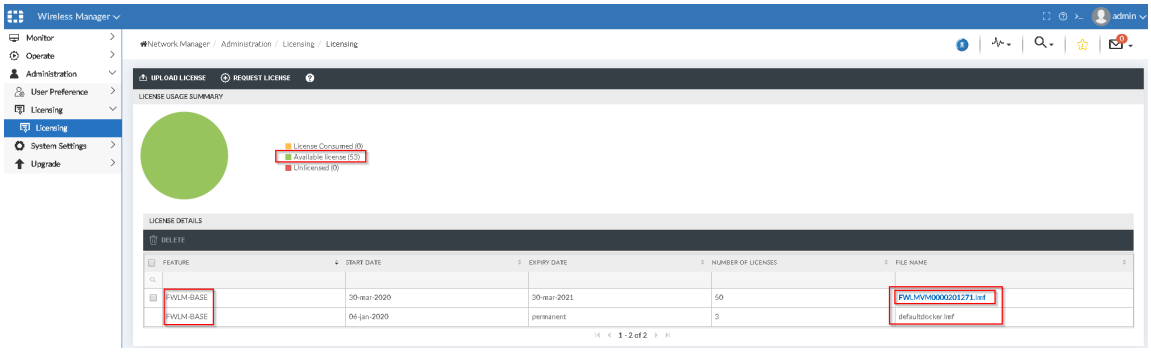


3. Click *Choose File*, select the license key, and then click *Upload*.

4. When the *File uploaded successfully* message is displayed, click *OK*.



The uploaded license is displayed.



Online update and verification for third-party certificates (OCSP stapling)

You can enable Anycast to optimize the routing performance to FortiGuard servers. Relying on Fortinet DNS servers, FortiManager obtains a single IP address for the domain name of each FortiGuard service. BGP routing optimization is transparent to FortiManager. The domain name of each FortiGuard service is the common name in that service's certificate. The certificate is signed by a third-party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, enabling FortiManager to always validate the FortiGuard server certificate efficiently.

This feature focuses on the Anycast option and TLS handshake using OCSP stapling when connecting to the FortiGuard server.

To enable online update and verification for third party certificates:

1. Enable Anycast support:

```
config fmupdate fds-setting
   set fortiguard-anycast enable
   set fortiguard-anycast-source {aws | fortinet}
end
```

When Anycast is enabled, FortiManager only completes the TLS handshake with a FortiGuard server that provides a *good* OCSP status for its certificate. Any other status will result in a failed SSL connection. Also, FortiGuard enforces connection only over port 443.

FortiManager connecting to FortiGuard:

1. FortiManager embeds CA bundle that includes third party intermediate CA and the root CA.
2. FortiManager finds FortiGuard IP address from the DNS.
3. FortiManager initiates TLS handshake with the FortiGuard IP address.
4. FortiGuard servers provide certificates with its OCSP status: good, revoked, or unknown.
5. FortiManager verifies CA against the root CA within the CA bundle.
6. FortiManager then verifies the intermediate CA's revoke status against the root CA's CRL.
7. Finally, FortiManager verifies the FortiGuard certificate OCSP status.

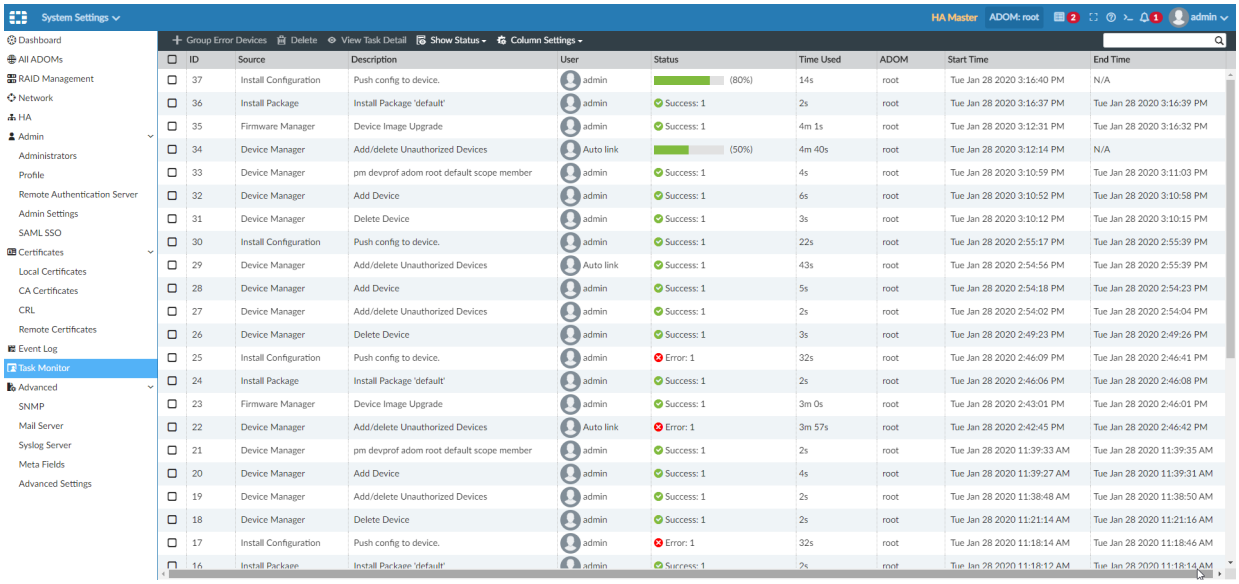
OCSP stapling is reflected on the signature interval (currently, 24 hours), and good means that the certificate is not revoked at that timestamp. The FortiGuard servers query the CA's OCSP responder every four hours and updates its OCSP status. If the FortiGuard server is unable to reach the OCSP responder, it keeps the last known OCSP status for seven days. This cached OCSP status is immediately sent out when a client connection request is made, which optimizes the response time.

Model device auto-link feature enhancements

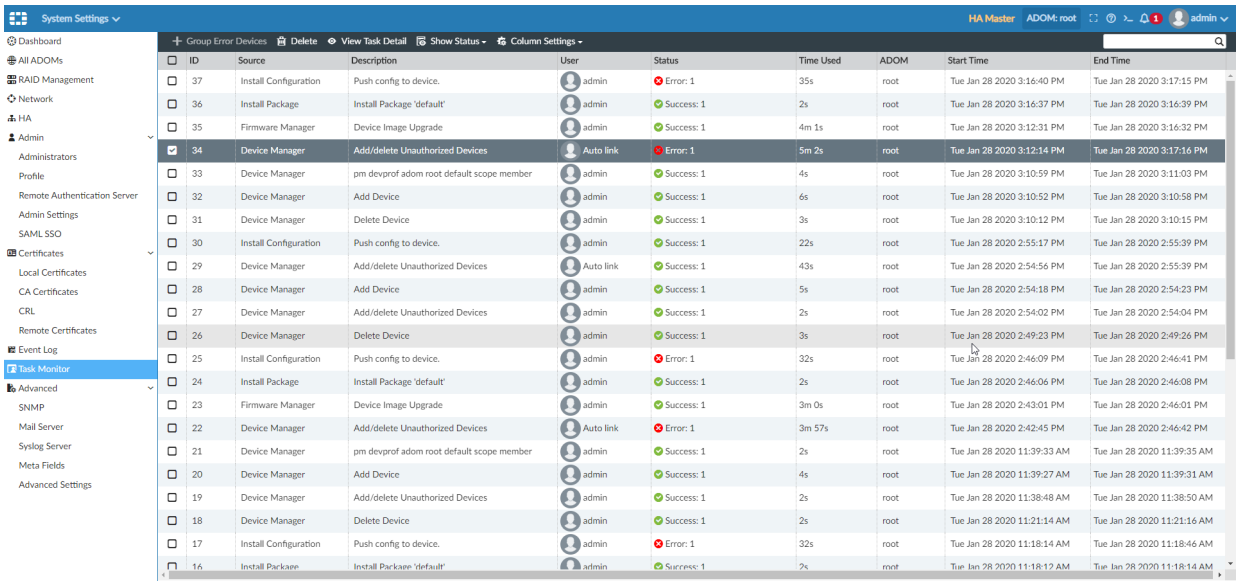
The *Task Monitor* displays more details about the task status and the amount of time to complete tasks. You can also filter the items in the *Task Monitor* pane and the *View History* window.

To view the task monitor in the GUI:

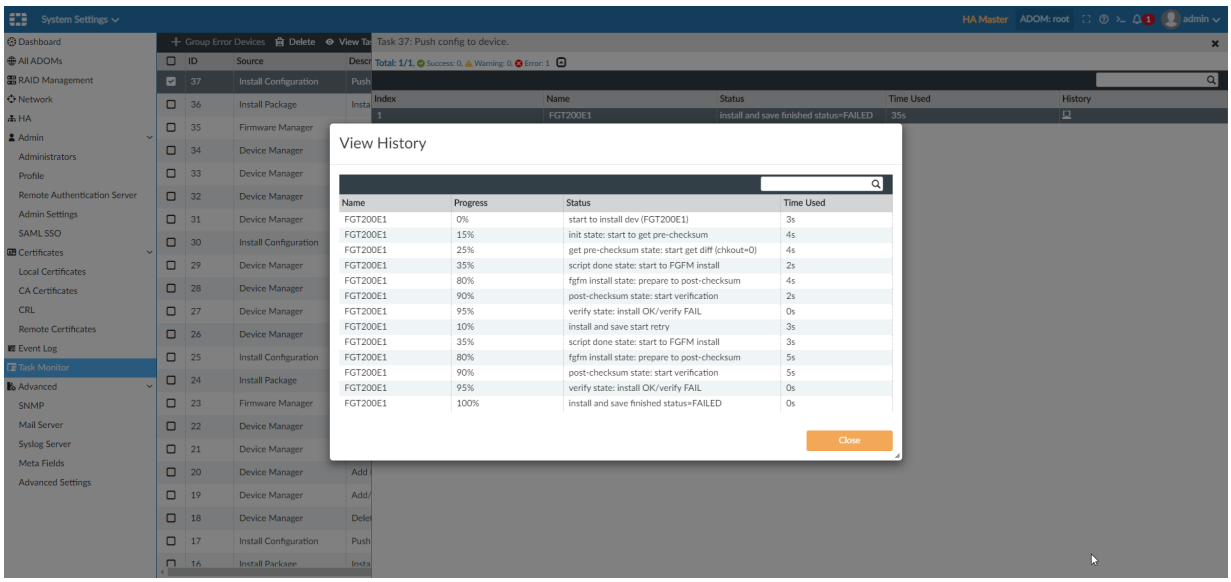
1. Go to *System Settings* > *Task Monitor*.
   The *Status* column displays a progress bar when a task is in progress. The *Time Used* column shows the amount of time used to complete the task.



   The column also includes a status description as well as the number of tasks associated with the item.

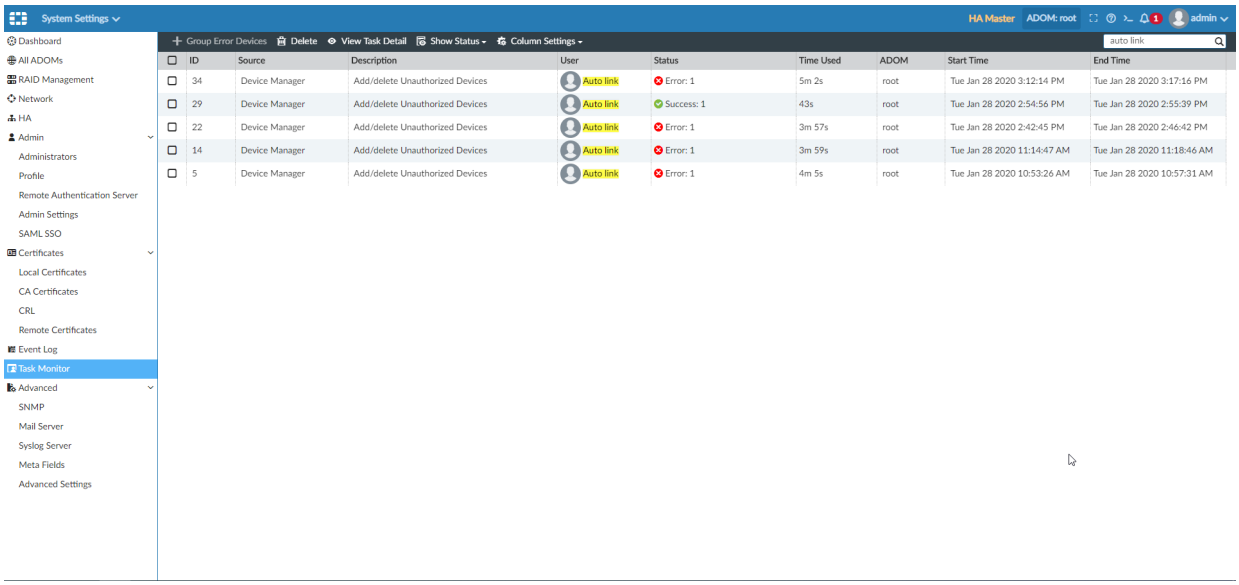


2. View the task history.
   a. Double-click an item in the *Task Monitor* pane. The task window opens.
   b. Click the icon in the *History* column. The *View History* window opens. To filter the content, enter a term in the search field.



   c. Click *Close*.

3. You can also filter the content in the *Task Monitor* pane by entering a term in the search field.



Interface-based shaping profiles and monitoring

The traffic monitor now supports interface-based shaping profiles.

The traffic shaping profiles feature is available for central management and per-device management of SD-WAN networks. It is available for ADOM versions 6.2 and 6.4.

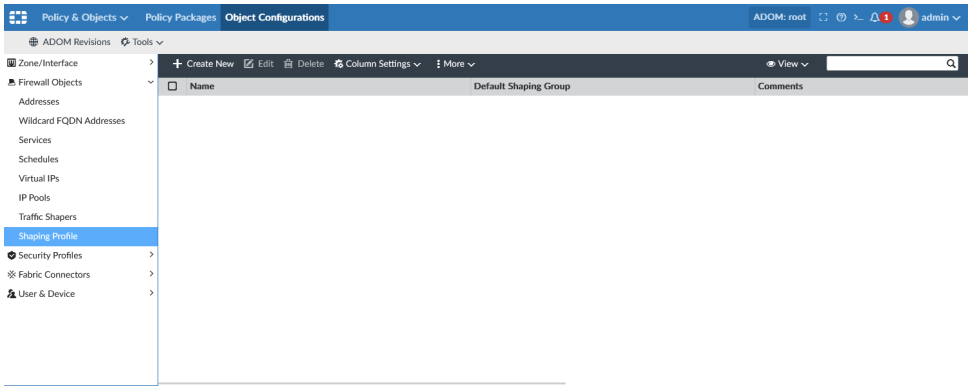
This topic contains the following sections:

Configuring traffic shaping profiles

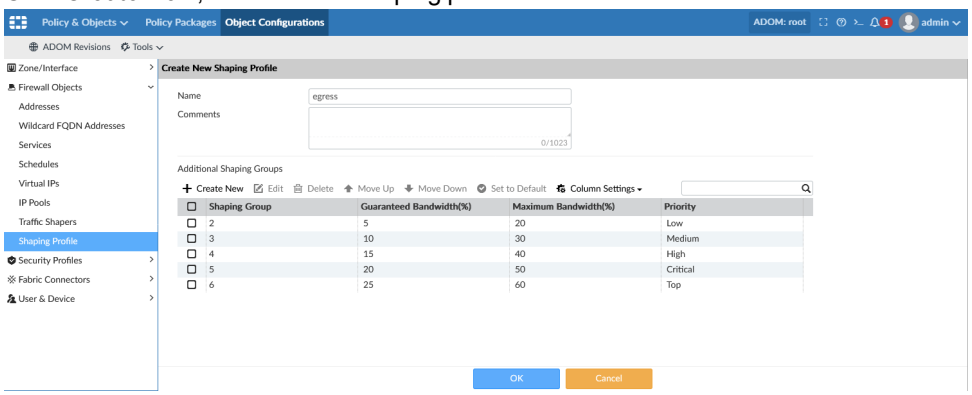
This procedure assumes that you have already configured an SD-WAN network. In order to use traffic shaping profiles, you must perform a number of steps before you can install traffic shaping profiles via a policy package to FortiGate devices in an SD-WAN network.

To configure traffic shaping profiles:

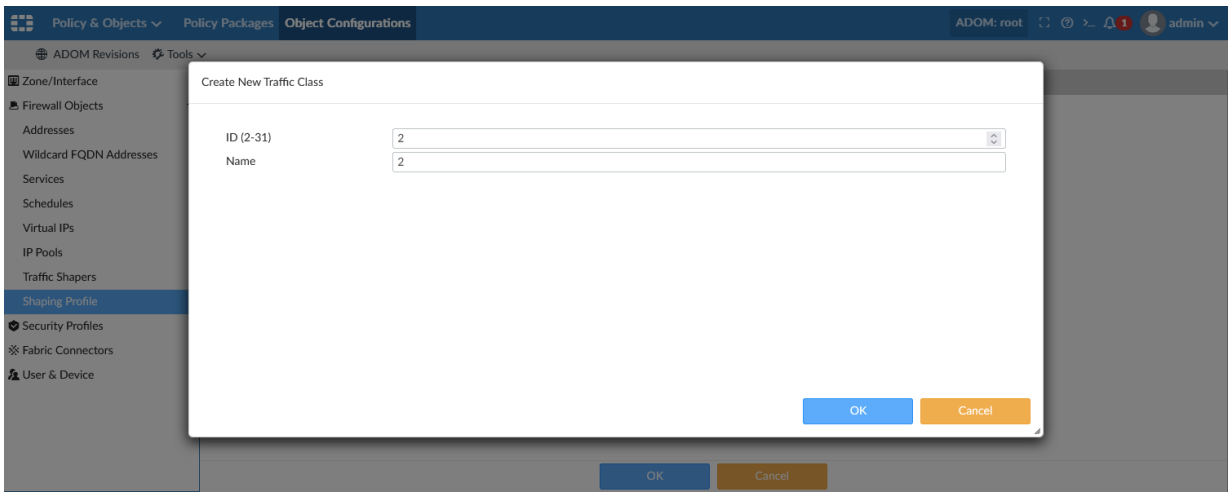
1. Configure shaping profiles:
   a. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Shaping Profile*.



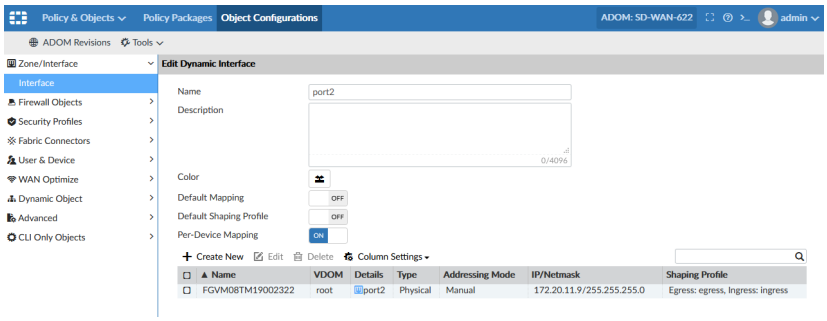
   b. Click *Create New*, and create a shaping profile.



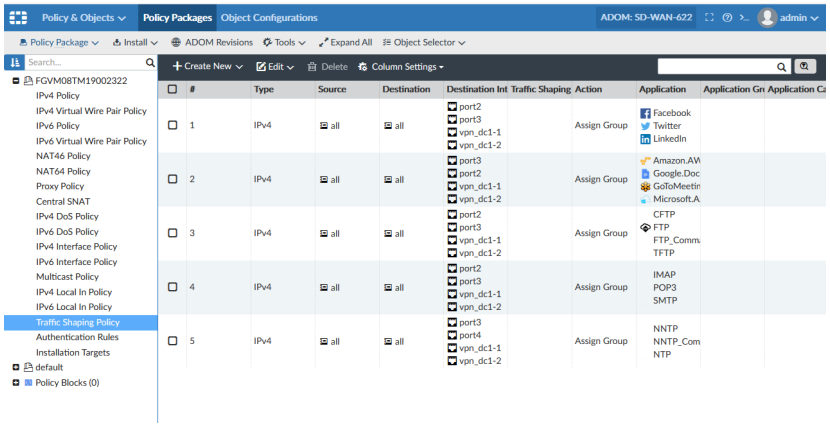
2. Create shaping groups and traffic shaping class ID.
   a. Click *Create New* in the *Additional Shaping Groups* table.
   b. Configure the *Guaranteed Bandwidth*, *Maximum Bandwidth*, and *Priority* for the shaping group.
   c. Click the *Traffic Shaping Class ID* dropdown and select a traffic class, or click the *Add* button to create a new traffic class.



3. Assign shaping profiles to interfaces:
   a. Go to *Policy & Objects* > *Object Configurations* > *Zone/Interface* > *Interface*.
   b. In the content pane, double-click an interface to open it for editing.
   c. Map the shaping profile to a device or group.

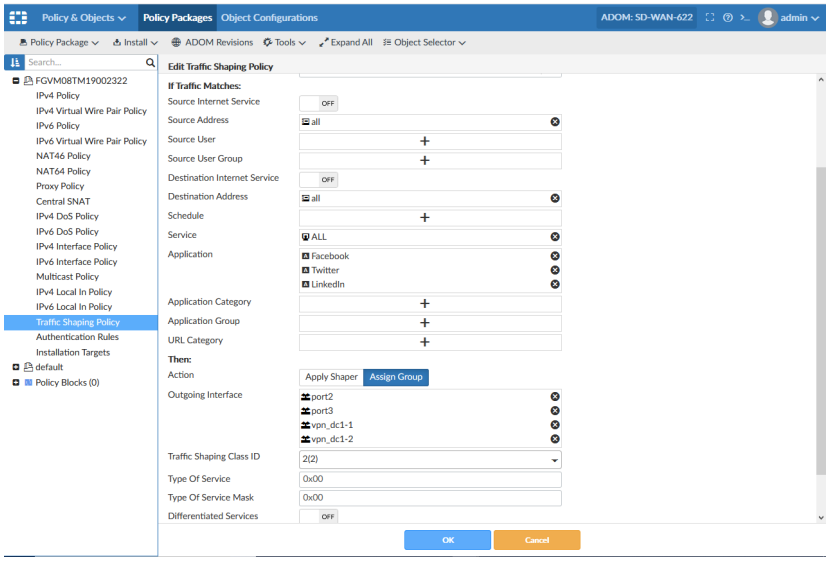


4. Create an IPv4 policy for the SD-WAN network.
5. Create a traffic shaping policy:
   a. Go to *Policy & Objects* > *Policy Packages* > *Traffic Shaping Policy*.
   The traffic shaping policies are displayed.



   b. Click *Create New*.
   c. Select *Assign Group* as the *Then* > *Action*, and in the *Traffic Shaping Class ID* box, select the class ID object

that you created, and set the remaining options as desired.

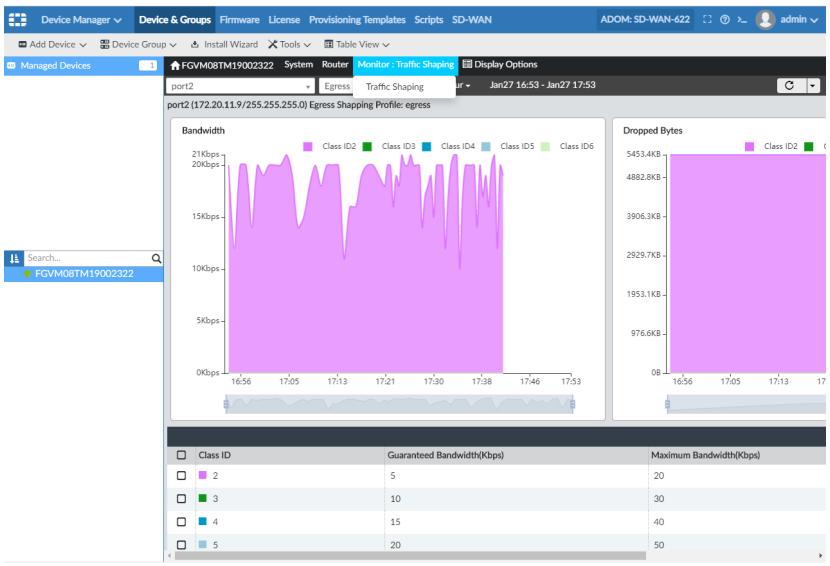


6. Install the IPv4 and traffic shaping policies to the FortiGate devices in the SD-WAN network.
   After the policies are installed, you can use monitor traffic shaping.

Monitoring traffic shaping

To monitor traffic shaping:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree menu, select the device group, for example, *Managed Devices*.
   The list of devices display in the content pane and in the bottom tree menu.
3. In the bottom tree menu, select a device.
   The *System:* Dashboard for the device displays in the content pane.
4. Go to *Monitor: Traffic Shaping*. This option may need to be enabled in *Display Options* before it is available.
   Graphs of *Bandwidth* and *Dropped Bytes* are displayed. Below the graphs you can view the *Class ID*, *Guaranteed Bandwidth(Kbps)*, *Maximum Bandwidth(Kbps)*, and *Application*.



5. Select a different port from the list.
   The graphs and information update.
6. Change the refresh interval between *every 5/10/15/20/30 minutes* or *Manual Refresh*.
7. You can enable or disable data history by using the CLI.

   ```
   config system admin setting
      set sdwan-monitor-history enable/disable
   end
   ```

   By default, `sdwan-monitor-history` is set to `disable`, and you can view the last 10 minutes data of data. The request/response data is retrieved directly from FortiGate. You can check `/var/rtm/history` for log files.

   When you set `sdwan-monitor-history` to `enable`, you can view data for last 24/12/6/1/N hours, or you can customize the time up to a maximum of 180 days. You can check `/var/rtm/history` for log files to be appended every 5 minutes.

In 6.4.3 and later, the traffic shaping monitor can be added as a widget in the device database's *Dashboard* page.

Configuring traffic shaping with the CLI

This procedure assumes that you have already configured an SD-WAN network.

To configure traffic shaping with the CLI:

1. Create traffic class objects:

   ```
   config firewall traffic-class
   edit 2
   set class-name "2"
   next
   edit 3
   set class-name "3"
   next
   edit 4
   ```

```
set class-name "4"
next
edit 5
set class-name "5"
next
edit 6
set class-name "6"
next
end
```

2. Configure shaping profiles:
   Use the class ID created in the previous step.

```
config firewall shaping-profile
edit "egress"
set default-class-id 2
config shaping-entries
edit 1
set class-id 2
set priority low
set guaranteed-bandwidth-percentage 5
set maximum-bandwidth-percentage 20
next
edit 3
set class-id 3
set priority medium
set guaranteed-bandwidth-percentage 10
set maximum-bandwidth-percentage 30
next
edit 4
set class-id 4
set guaranteed-bandwidth-percentage 15
set maximum-bandwidth-percentage 40
next
edit 2
set class-id 5
set priority critical
set guaranteed-bandwidth-percentage 20
set maximum-bandwidth-percentage 50
next
edit 5
set class-id 6
set priority top
set guaranteed-bandwidth-percentage 25
set maximum-bandwidth-percentage 60
next
end
next
edit "ingress"
set default-class-id 3
config shaping-entries
edit 1
set class-id 3
set priority medium
set guaranteed-bandwidth-percentage 30
set maximum-bandwidth-percentage 50
next
edit 2
```

```
set class-id 5
set guaranteed-bandwidth-percentage 50
set maximum-bandwidth-percentage 80
next
end
next
end
```

3. Assign shaping profiles to interfaces:
   Use the shaping profile created in the previous step.

```
config system interface
...
edit "port2"
set vdom "root"
set ip 172.20.11.9 255.255.255.0
set allowaccess ping https ssh http
set type physical
set inbandwidth 100
set outbandwidth 100
set egress-shaping-profile "egress"
set estimated-upstream-bandwidth 15000
set estimated-downstream-bandwidth 15000
set role wan
set snmp-index 2
set ingress-shaping-profile "ingress"
next
edit "port3"
set vdom "root"
set ip 172.20.12.9 255.255.255.0
set allowaccess ping ssh
set type physical
set inbandwidth 500
set outbandwidth 500
set egress-shaping-profile "egress"
set estimated-upstream-bandwidth 500
set estimated-downstream-bandwidth 500
set role wan
set snmp-index 3
set ingress-shaping-profile "ingress"
next
...
edit "vpn_dc1-1"
set vdom "root"
set ip 10.254.30.2 255.255.255.255
set allowaccess ping
set type tunnel
set egress-shaping-profile "egress"
set remote-ip 10.254.30.1 255.255.255.0
set estimated-upstream-bandwidth 100
set estimated-downstream-bandwidth 50
set role wan
set snmp-index 113
set interface "port2"
set ingress-shaping-profile "ingress"
next
edit "vpn_dc1-2"
set vdom "root"
```

```
set ip 10.254.31.2 255.255.255.255
set allowaccess ping
set type tunnel
set remote-ip 10.254.31.1 255.255.255.0
set estimated-upstream-bandwidth 15000
set estimated-downstream-bandwidth 500
set role wan
set snmp-index 114
set interface "port3"
next
end
```

4. Create an IPv4 policy for the SD-WAN network.
5. Create a traffic shaping policy:

```
Use the class ID created in previous steps.
config firewall shaping-policy
edit 1
set name "default"
set service "ALL"
set application 15832 16001 16331
set dstintf "port2" "port3" "vpn_dc1-1"
set class-id 2
set srcaddr "all"
set dstaddr "all"
next
edit 2
set name "shaping-ftp"
set service "ALL"
set application 27210 16541 16354 38924
set dstintf "port3" "port2" "vpn_dc1-1"
set class-id 3
set srcaddr "all"
set dstaddr "all"
next
edit 3
set name "http"
set service "ALL"
set application 16365 15896 152305673 16253
set dstintf "port2" "port3" "vpn_dc1-1"
set class-id 4
set srcaddr "all"
set dstaddr "all"
next
edit 4
set name "5"
set service "ALL"
set application 16103 16104 16074
set dstintf "port2" "port3" "vpn_dc1-1"
set class-id 5
set srcaddr "all"
set dstaddr "all"
next
edit 5
set name "6"
set service "ALL"
set application 16213 152305672 16270
set dstintf "port3" "port4" "vpn_dc1-1"
```

```
    set class-id 6
    set srcaddr "all"
    set dstaddr "all"
    next
    end
```

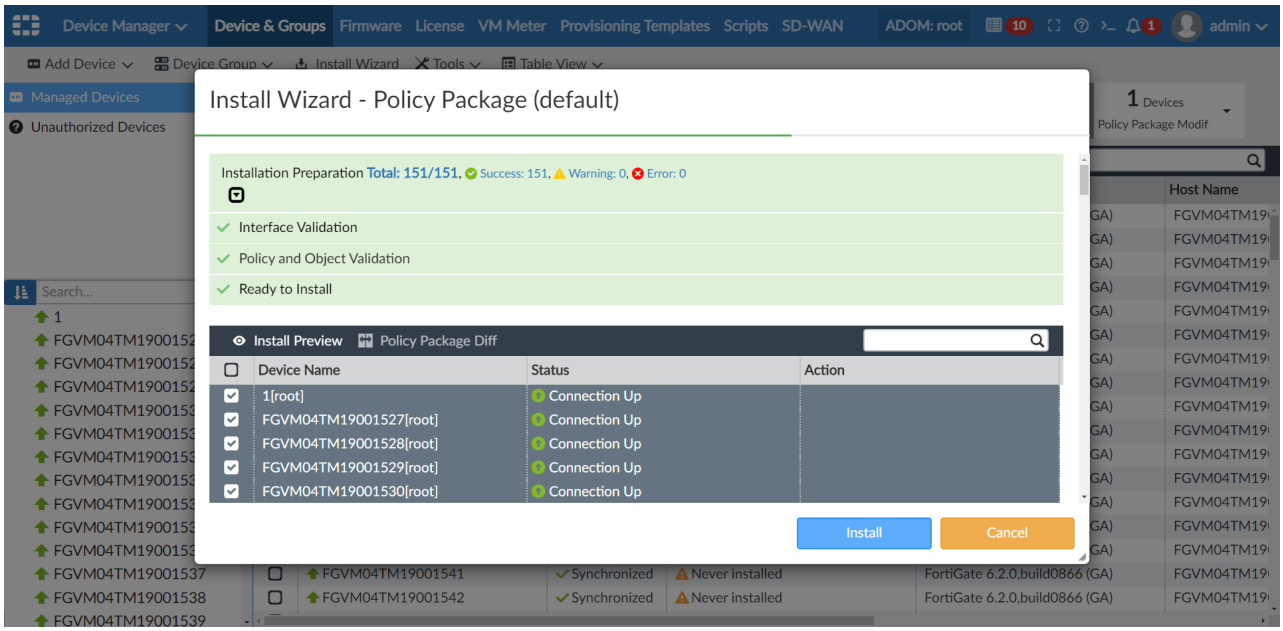
6. Install the IPv4 and traffic shaping policies to the FortiGate devices in the SD-WAN network.
   After the policies are installed, you can use monitor traffic shaping.

Multiple device selection and consolidated install preview for policy package installation

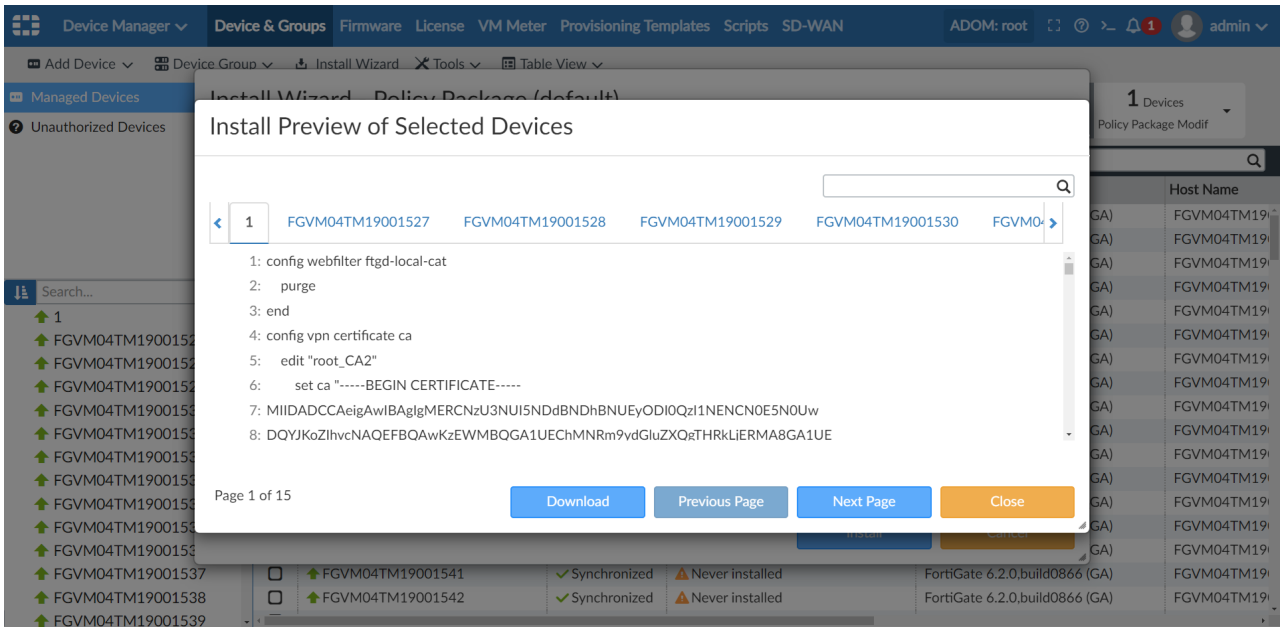
You can now preview a policy package and device settings in up to 10 devices when using the Install Wizard. Multiple device selection is available in the *Device Manager* and *Policy & Objects* tiles.

To preview multiple devices in Device Manager:

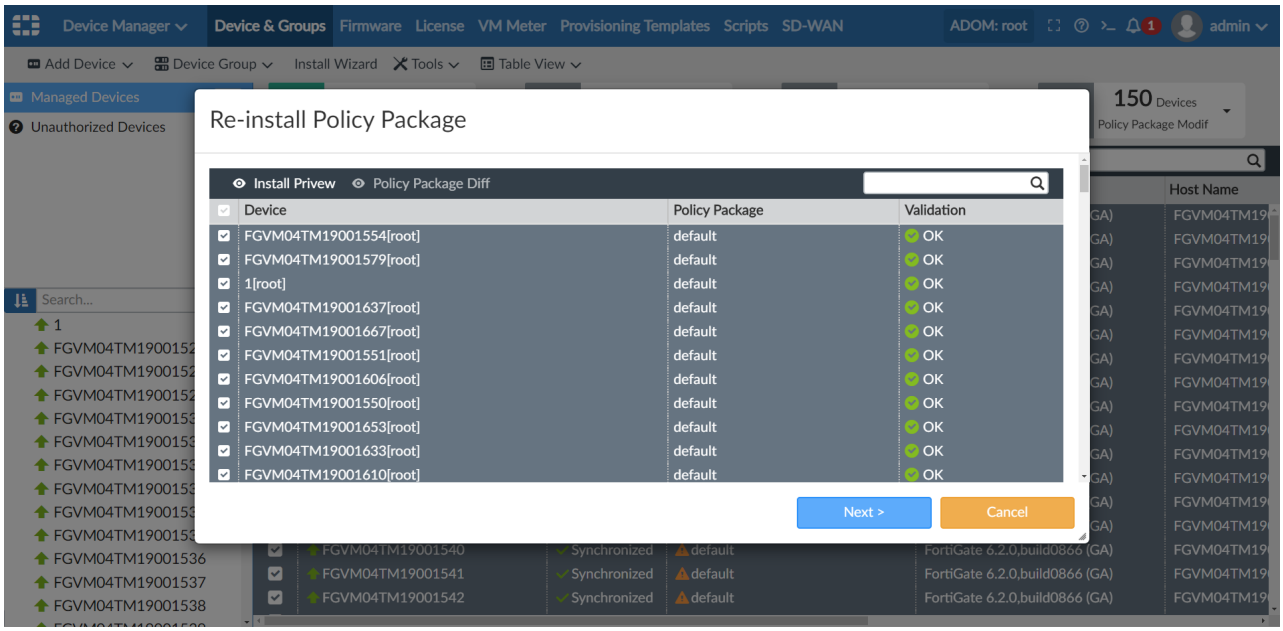
1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, click *Install Wizard*.
3. Select *Install Policy Package & Device Settings*, and then specify the policy package and other parameters. Click *Next*.
4. Select a maximum of 10 devices, and then click *Install Preview*.



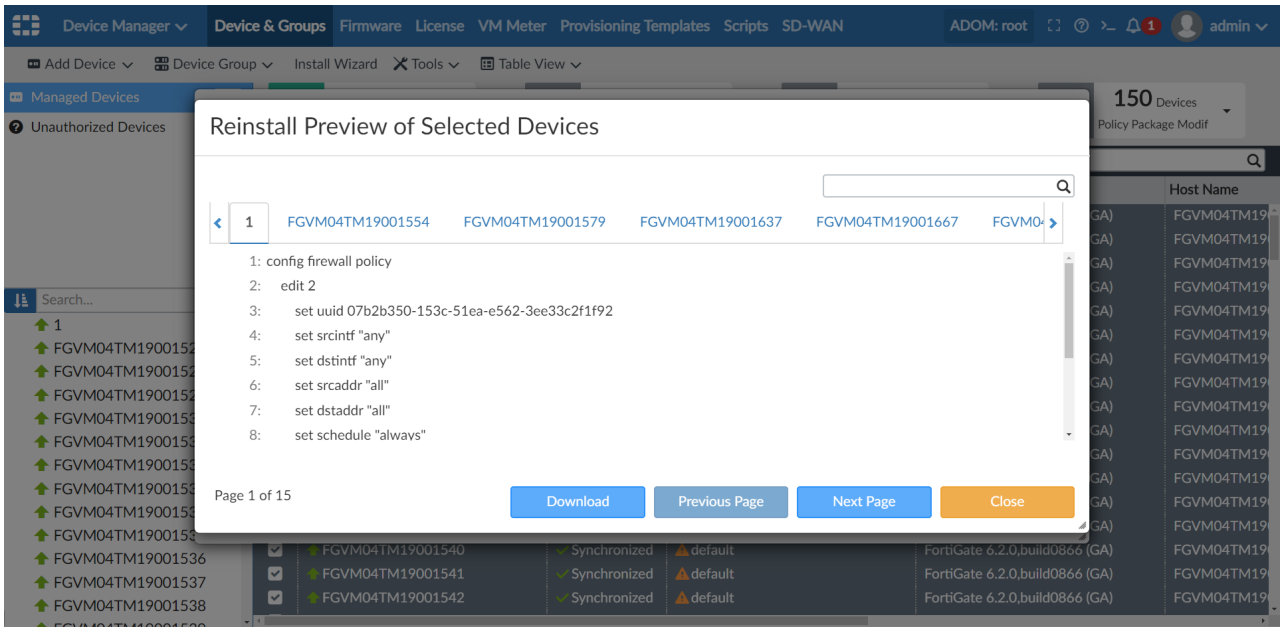
5. Click *Next Page* to preview the next 10 devices.



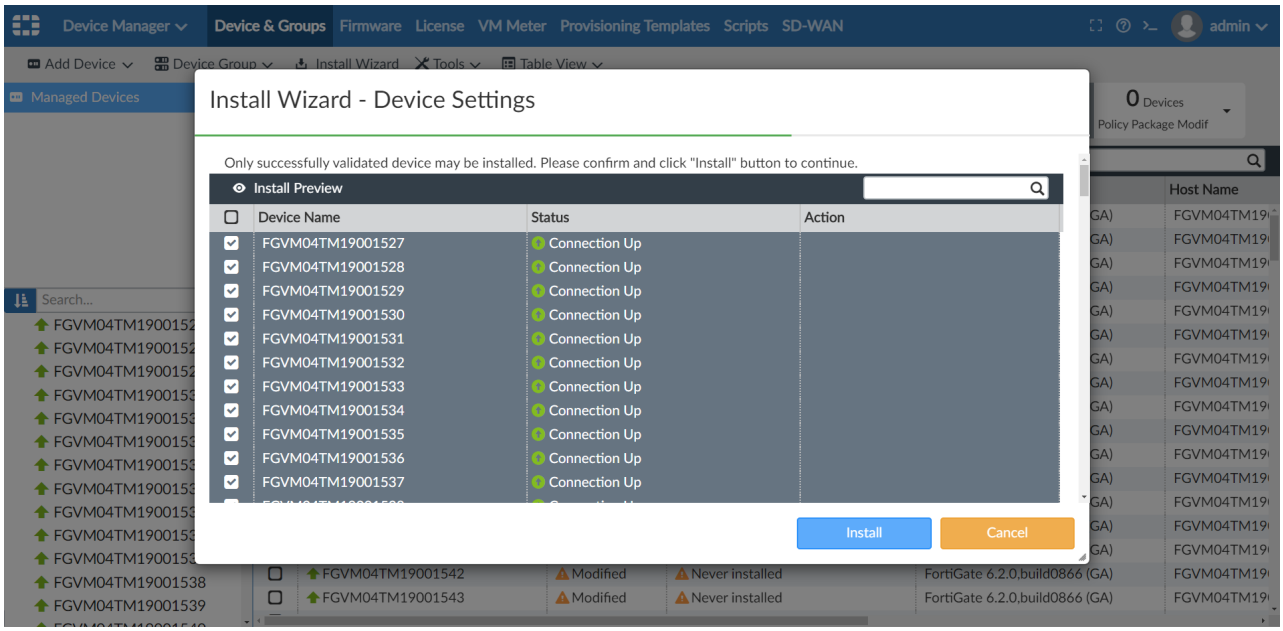
6. In the toolbar click *Install* > *Re-install Policy*.
   After data is gathered, the *Re-install Policy Package* window is displayed.
7. Select up to 10 devices, and then click *Install Preview*.



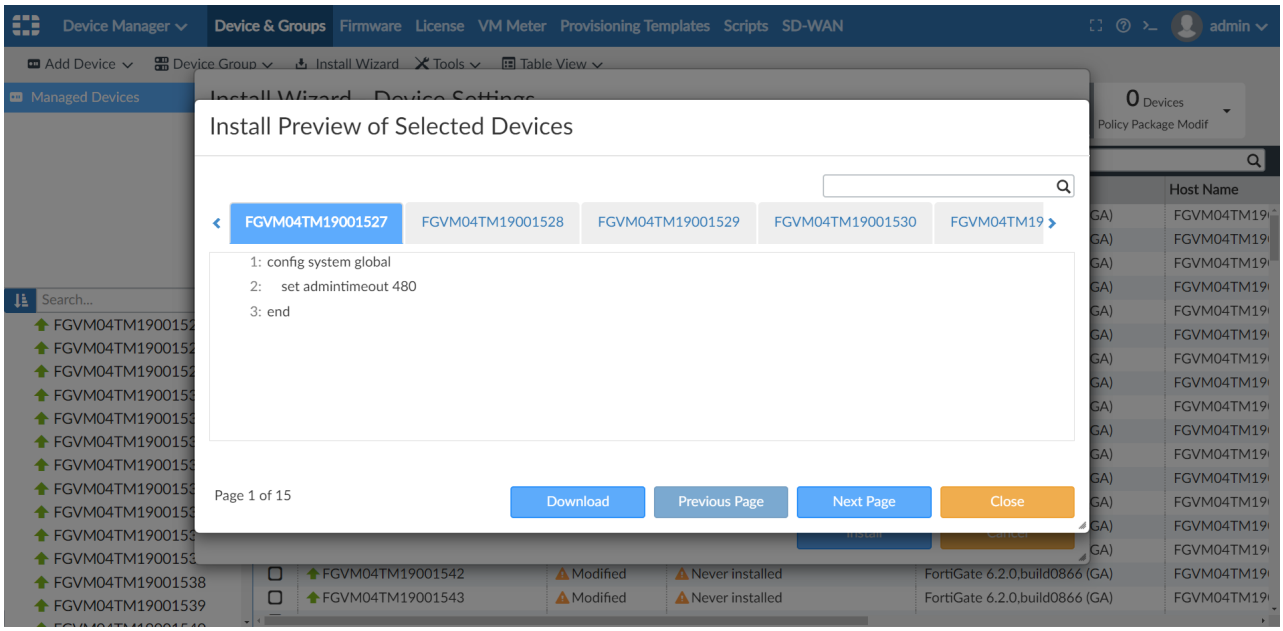
8. Click *Next Page* to preview the next 10 devices.



9. Multiple preview is also available in the *Install Wizard - Device Settings* window.

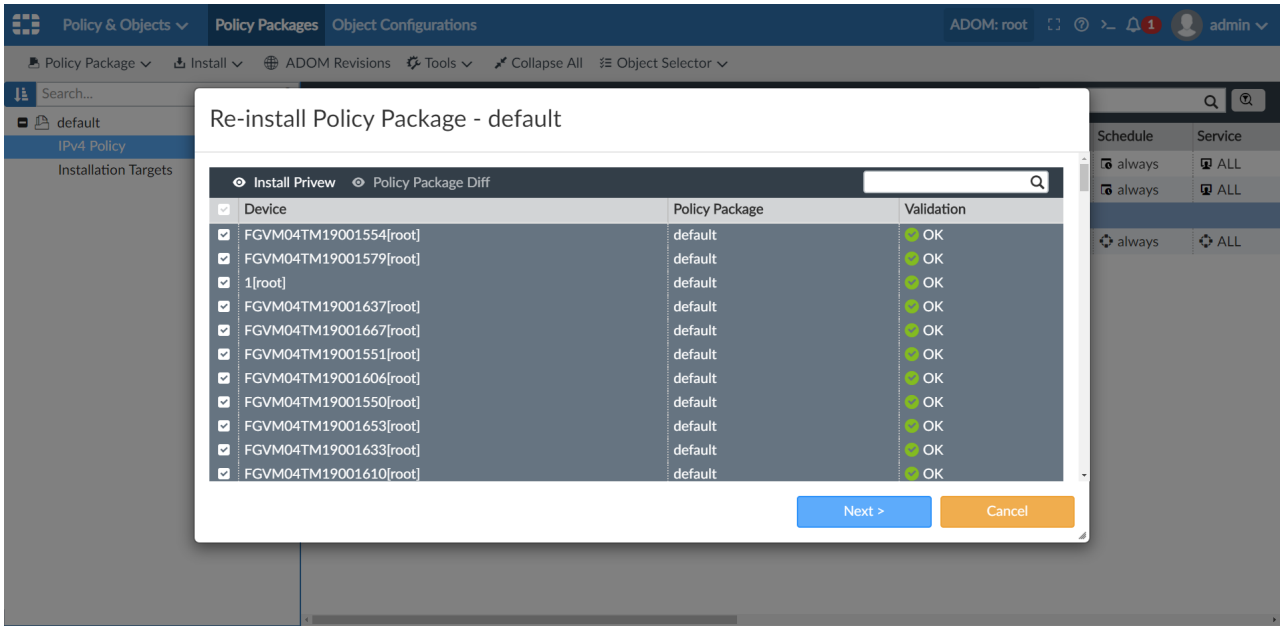


Click *Next Page* to preview the settings in the next 10 devices.

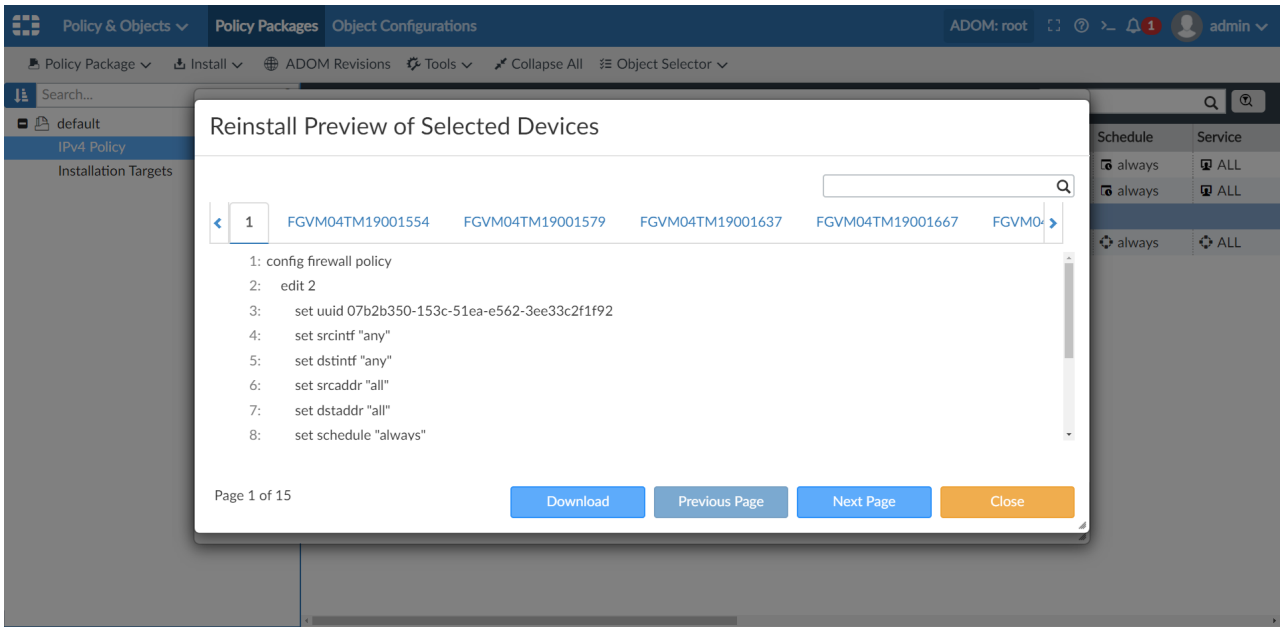


To preview multiple devices in Policy & Objects:

1. Go to *Policy & Objects* > *Policy Packages*, and then select a policy from the tree menu.
2. In the toolbar, click *Install* > *Re-Install Policy*. After data is gathered, the *Re-install Policy Package* window is displayed.
3. Select up to 10 devices, and then click *Install Preview*.



Click *Next Page* to preview the next 10 devices.



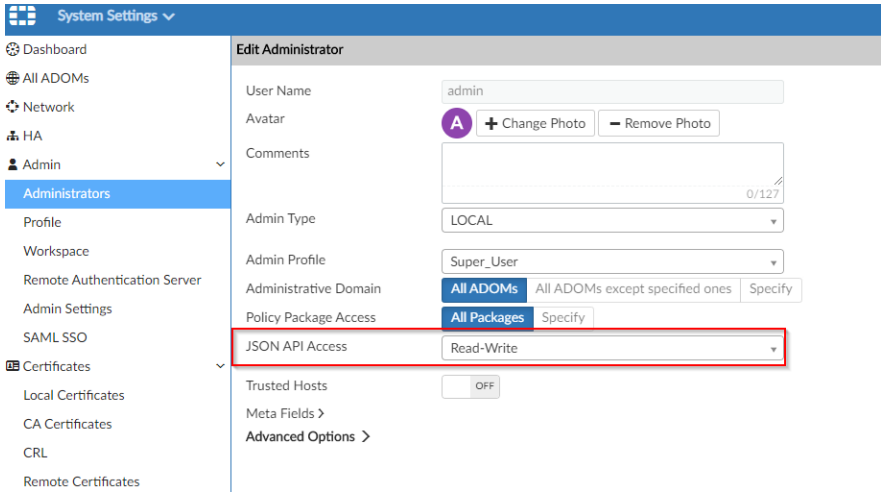
FortiManager detects an unauthorized FortiAP connected to a managed FortiGate

You can now authorize unknown APs that are connected to a managed FortiGate via FortiManager.

You must enable *JSON API access* to *Read-Write* to be able to authorize unknown FortiAP devices.

To enable read-write JSON API access:

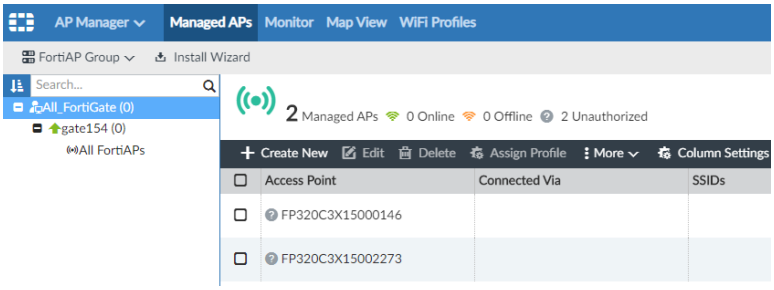
1. Go to *System Settings* > *Administrators*.
2. Double-click the *Admin* account to open it for editing.
   The *Edit Administrator* pane opens.



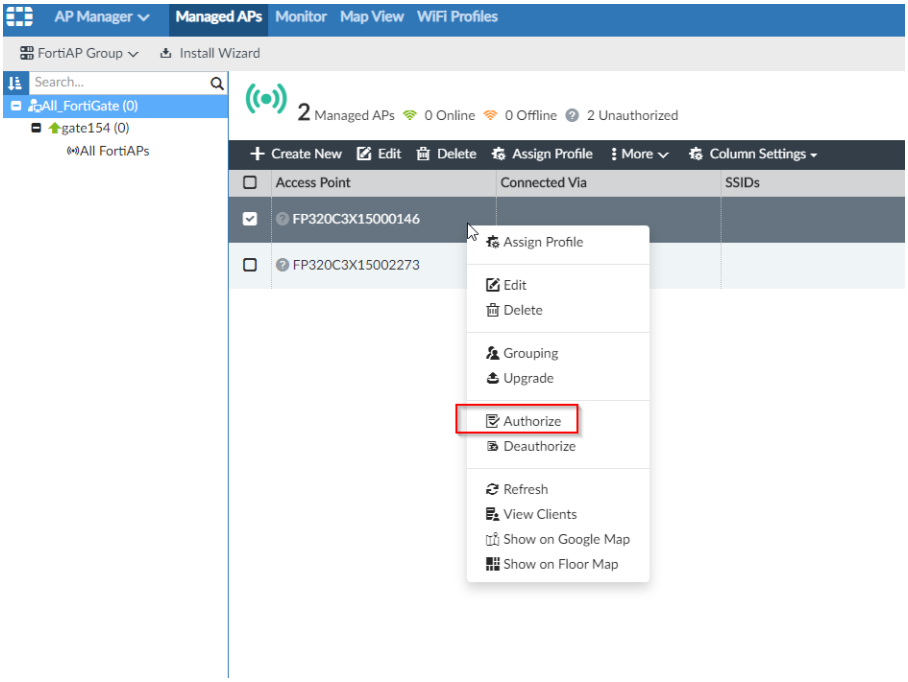
3. Beside *JSON API Access*, select *Read-Write*, and click *OK*.

To authorize unknown APs:

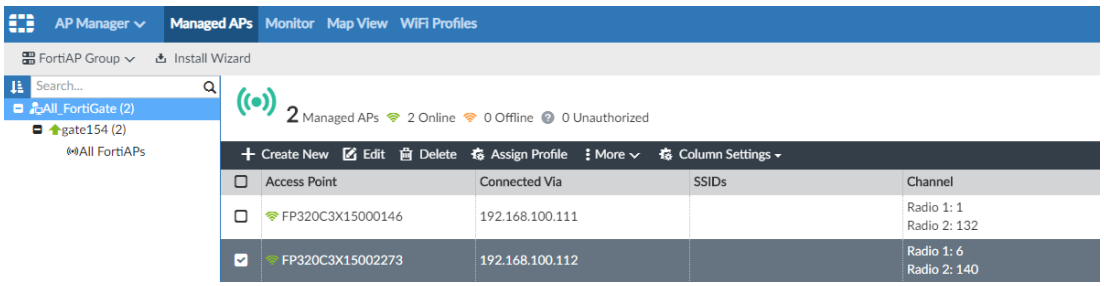
1. Go to *AP Manager* > *Managed APs*.
2. In the tree menu, select the group or FortiGate that contains the unknown FortiAP devices to be authorized.



3. Select the unknown FortiAP devices and either click *More* > *Authorize* from the toolbar, or right-click and select *Authorize*.



4. Wait awhile and then select the APs and click *More* > *Refresh*.
   APs are now online and displayed.

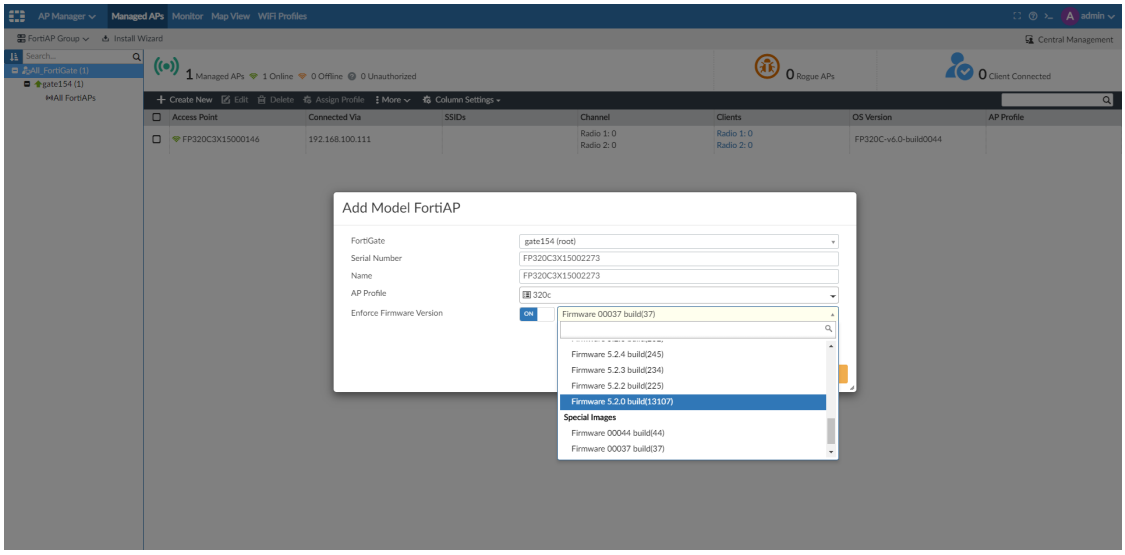


Enforce firmware version when on-boarding a new FortiAP

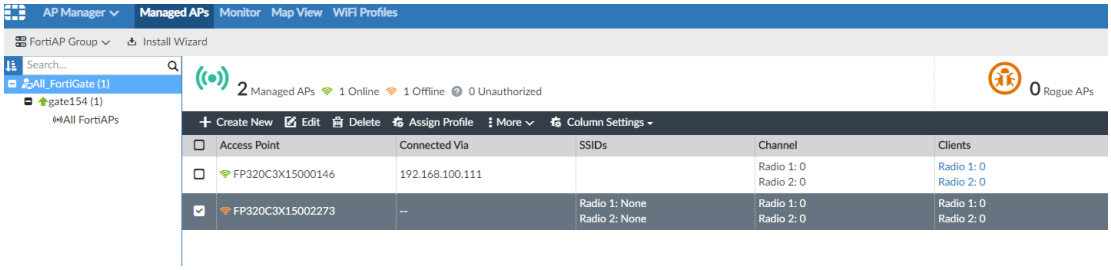
You can enforce a firmware version on a FortiAP device using FortiManager.

To enforce a firmware version:

1. Go to *AP Manager* > *Managed APs*.
2. Click *Create New* on the content pane toolbar. The *Add FortiAP* dialog box opens.

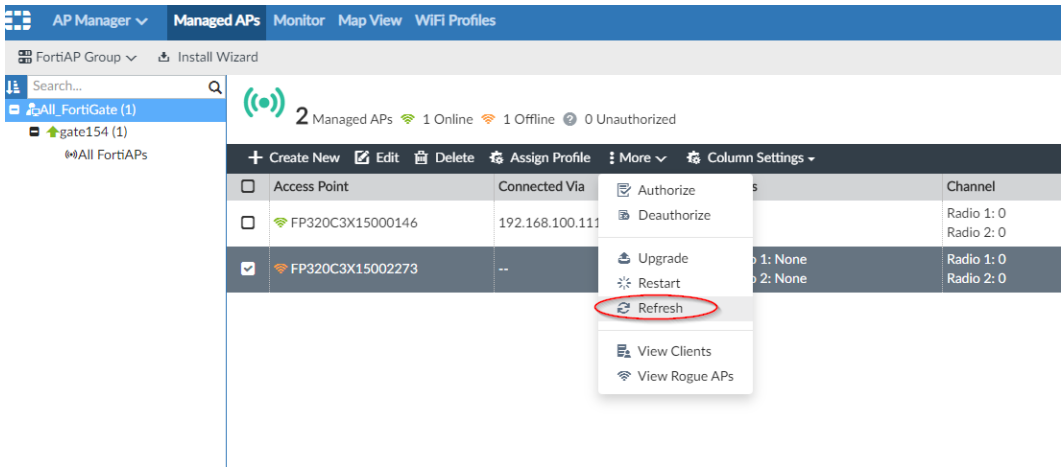


3. In the *Add FortiAP* dialog, configure the settings for your FortiAP device.
   Toggle *ON Enforce Firmware Version* to enforce a firmware version and select the firmware version from the drop-down menu.
4. Click *OK* to add your device.
5. In the tree menu under *AP Manager* > *Managed APs*, a model FortiAP device is created and added to the managed FortiGate.
   The model FortiAP is displayed as an offline authorized AP.

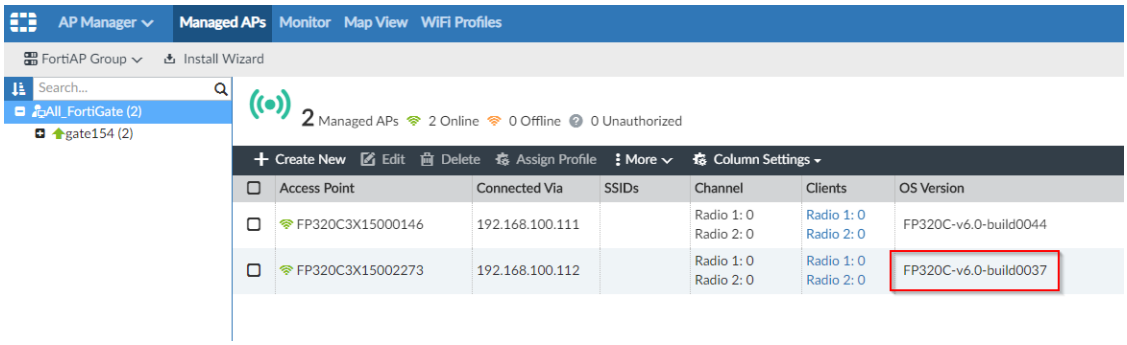


   Once the AP is connected to the FortiGate and appears online, wait around 10 minutes for the enforced firmware to be displayed.

6. Select the AP and click *More* from the toolbar and select *Refresh*.

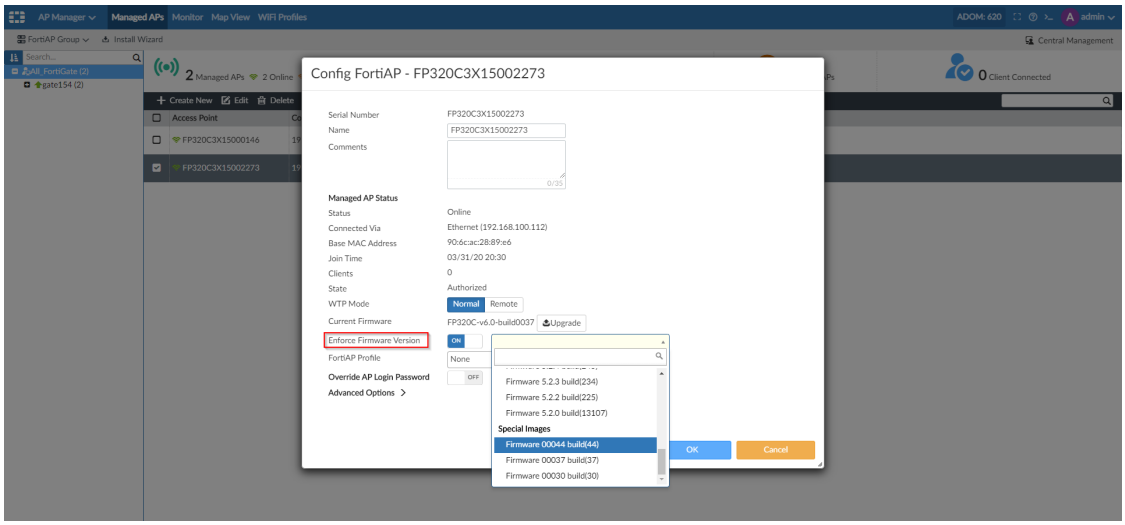


The AP is now online with the enforced firmware version.



To enforce a firmware version on an existing FortiAP device:

1. Go to *AP Manager* > *Managed APs*.
2. In the tree menu, select the group or FortiGate that contains the FortiAP device to be edited.
3. Locate the FortiAP device in the list in the content pane, or refine the list by selecting an option from the quick status bar.
4. Either select the FortiAP and click *Edit* from the toolbar, double-click on the FortiAP, or right-click on the FortiAP and select *Edit*. The *Config FortiAP* window opens.



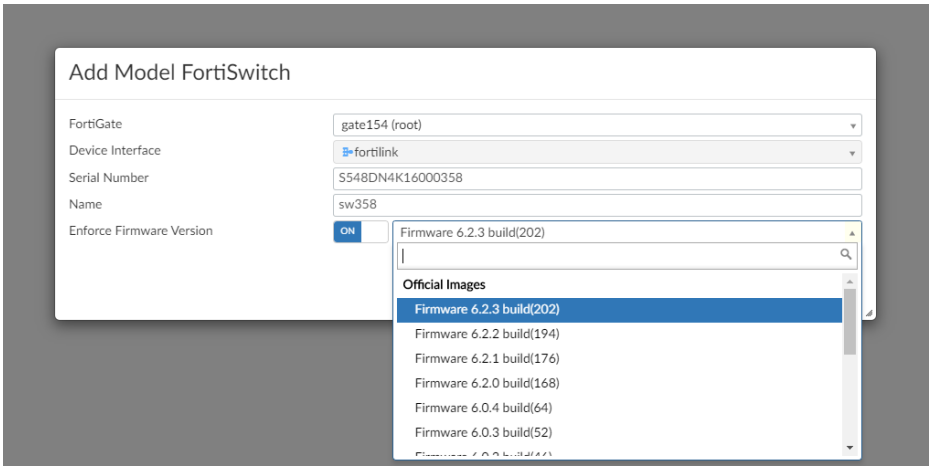
5. In the *Config FortiAP* window, edit the FortiAP to set firmware enforcement.
   Once the AP is online, FortiManager enforces the firmware version.

Enforce firmware version when on-boarding a new FortiSwitch

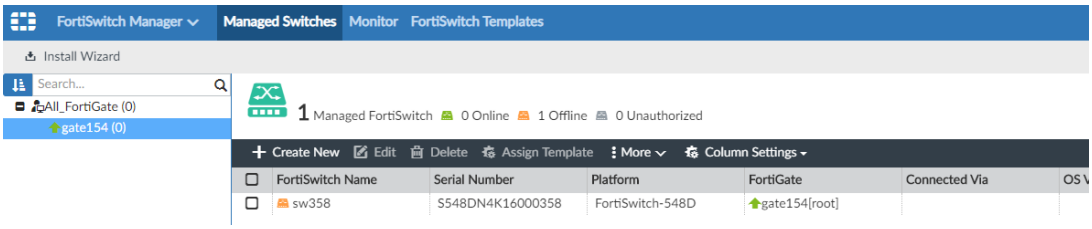
You can enforce a firmware version on a FortiSwitch using FortiManager.

To enforce a firmware version:

1. Go to *FortiSwitch Manager > Managed Switches*.
2. Click *Create New*. The *Add Model FortiSwitch* pane is displayed.

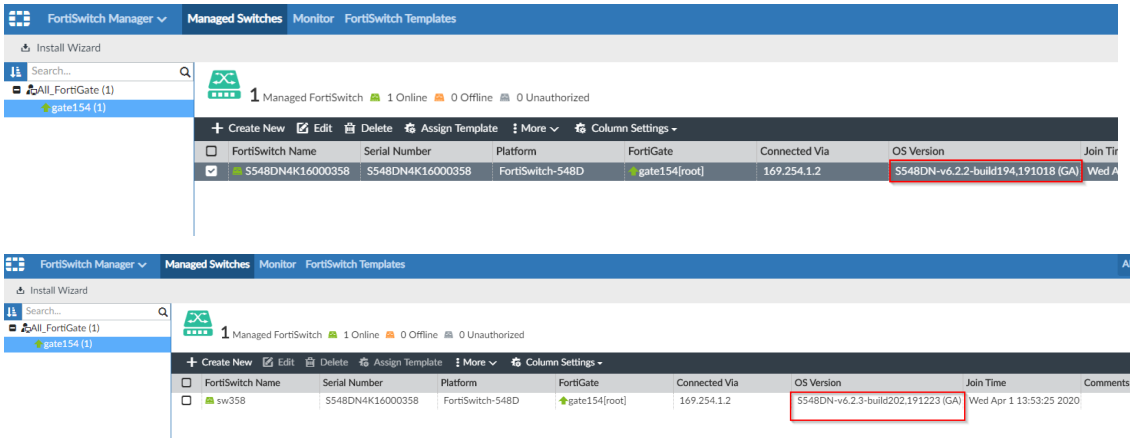


3. In the *Add Model FortiSwitch* dialog, configure the settings for your FortiSwitch.
   Toggle *ON Enforce Firmware Version* to enforce a firmware version and select the firmware version from the drop-down menu.
4. Click *OK* to add your FortiSwitch.
5. In the tree menu under *FortiSwitch Manager > Managed Switches*, a model FortiSwitch is created and added to the managed FortiGate.



When the FortiSwitch is online, FortiManager sets the firmware to the enforced version.

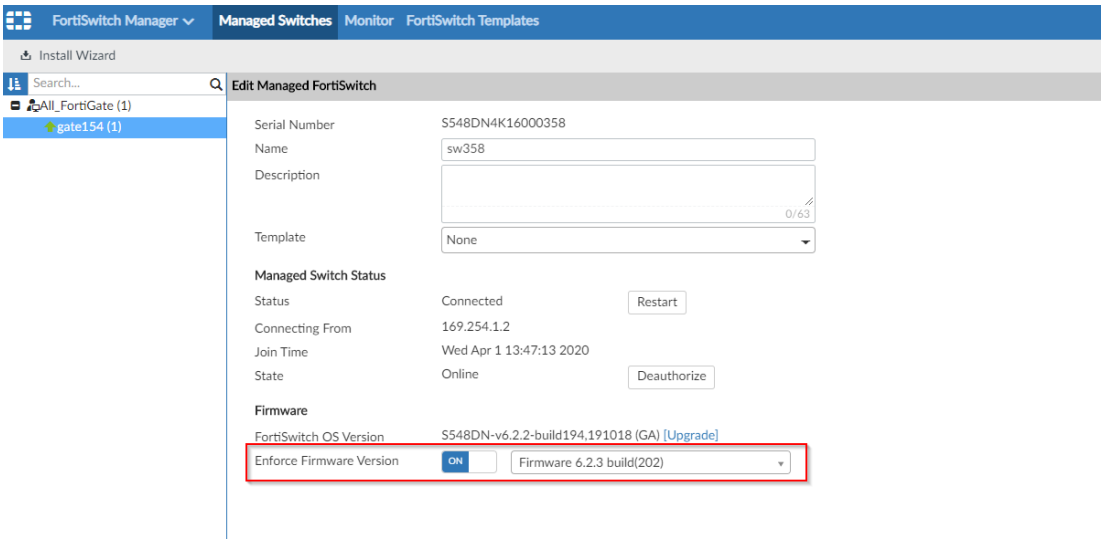
Here, the firmware is upgraded from the previous build 194 to build 202.



To enforce a firmware version on an existing FortiSwitch:

1. Go to *FortiSwitch Manager* > *Managed Switches*.
2. In the tree menu, select the FortiGate that contains the FortiSwitch device to be edited, or select *All_FortiGate* to list all of the switches.
3. Select the appropriate option from the quick status bar, and locate the switch in the content pane.
4. Double-click on the switch, select the switch and click *Edit* from the toolbar, or right-click on the switch and select *Edit*.

   The *Edit Managed FortiSwitch* window opens.



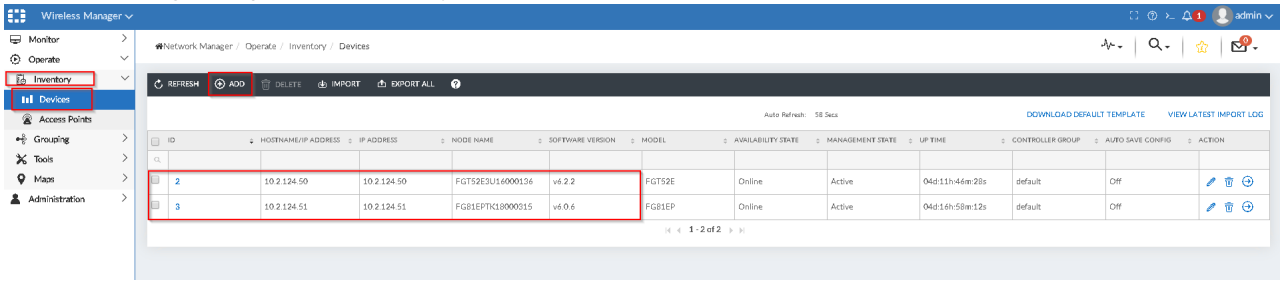
5. In the *Edit Managed FortiSwitch* window, edit the FortiSwitch to set firmware enforcement.
   Once the firmware is enforced, the FortiSwitch firmware will be changed to the enforced version.

Backup and restore FortiManager settings include Wireless Manager configuration

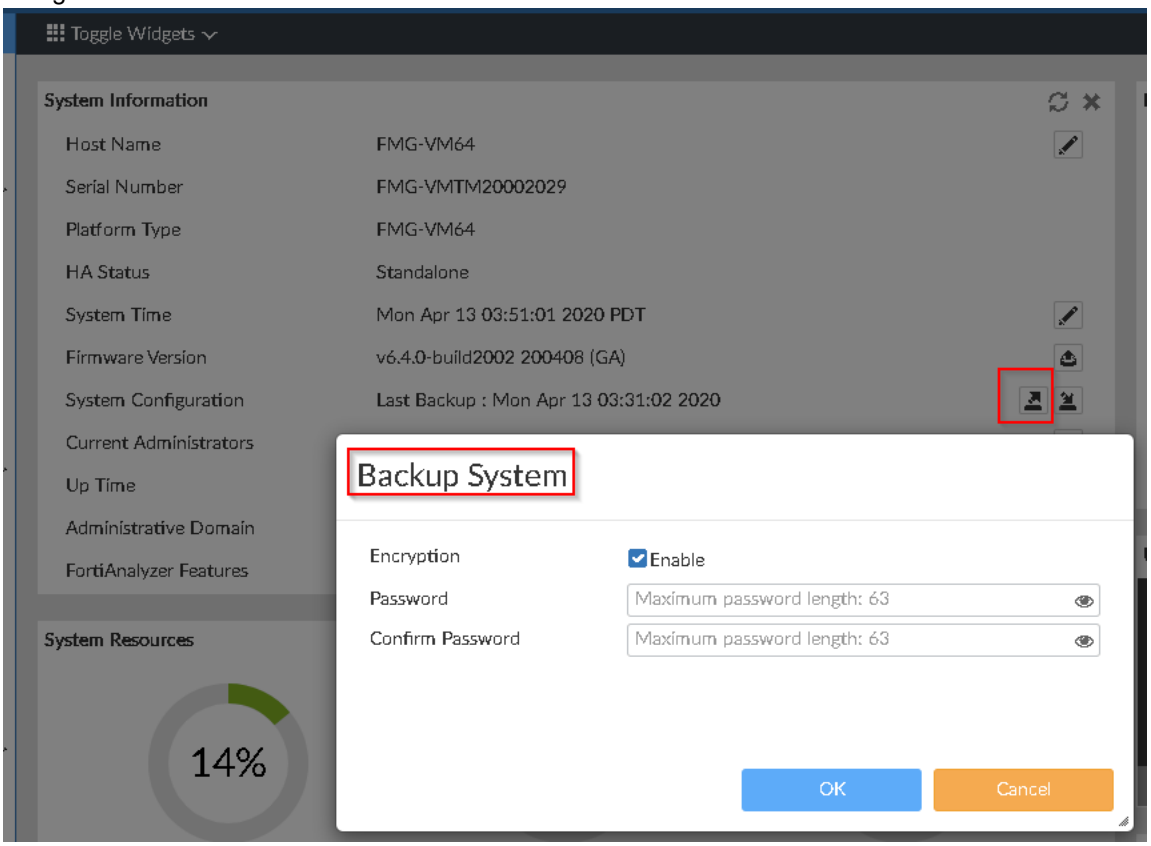
You can backup and restore FortiManager settings including Wireless Manager configuration using the GUI or CLI.

To backup and restore FortiManager settings along with Wireless Manager configuration using the GUI:

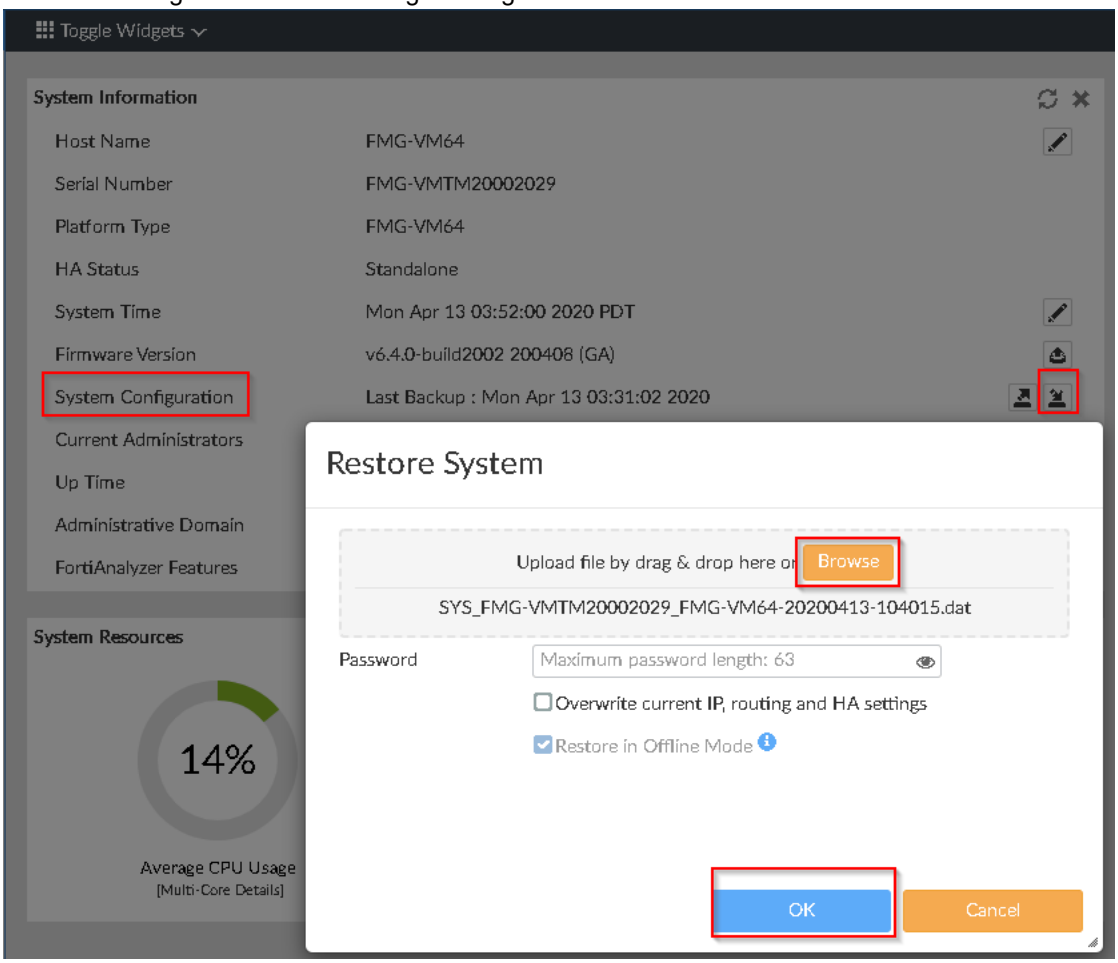
1. Ensure FortiGates are added to the Wireless Manager device inventory through *Management Extensions* > *Wireless Manager* > *Operate* > *Inventory* > *Devices*.



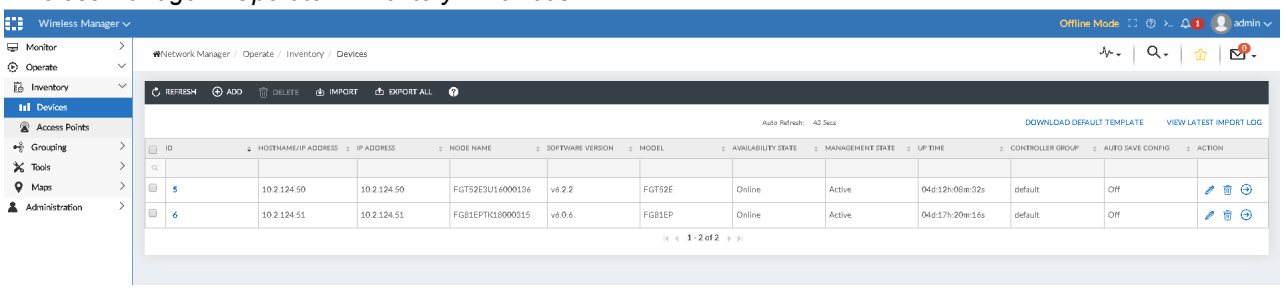
2. Navigate to the FortiManager *System Information* widget through *System Settings* > *Dashboard* and backup the system configuration. The FortiManager system configuration is backed up along with Wireless Manager configuration.



3. To restore the backed up settings, navigate to the FortiManager *System Information* widget through *System Settings* > *Dashboard* and restore the FortiManager system configuration. The FortiManager system configuration is restored along with Wireless Manager configuration.



4. Verify that the FortiGates are restored to the Wireless Manager device inventory through *Management Extensions* > *Wireless Manager* > *Operate* > *Inventory* > *Devices*.



To backup and restore FortiManager settings along with Wireless Manager configuration using the CLI:

1. To back up all the settings:

```
execute backup all-settings
```

2. To restore all the settings:

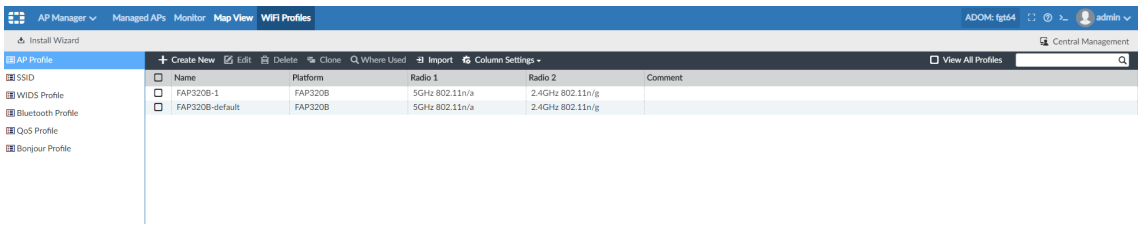
```
execute restore all-settings
```

Central SD-WAN, FortiAP, and FortiSwitch templates included in ADOM revision

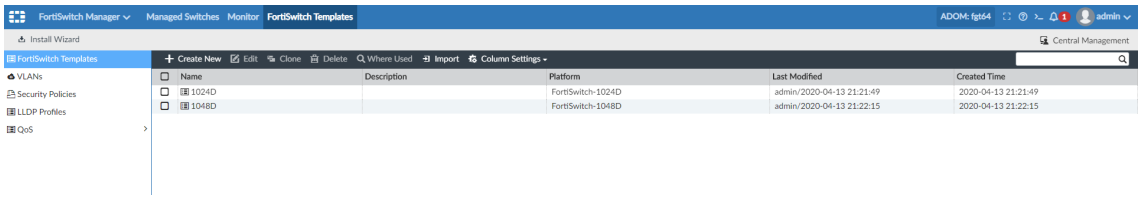
ADOM revisions now include SD-WAN templates, FortiAP profiles, and FortiSwitch templates when cetnral management for each is enabled. Previously ADOM revisions included only global policies, policy packages, and policy objects.

To include templates in ADOM revisions:

1. In the ADOM, ensure that central management is enabled for FortiAP, SD-WAN, and FortiSwitch.
   a. Go to *System Settings* > *All ADOMs*.
   b. Double-click the ADOM to open it for editing.
   c. Beside *Central Management*, select the checkbox for *FortiAP*, *SD-WAN*, and *FortiSwitch*.
   d. Click *OK*.
   Central management is enabled for FortiAP, SD-WAN, and FortiSwitch.
2. Create a profile or template for FortiAP, SD-WAN, and FortiSwitch.
   The following example describes how to create a profile for FortiAP.
   a. Go to *AP Manager* > *WiFi Profiles*.
   b. In the content pane, click *Create New*.
   c. Complete the options, and click *OK*.
   The profile is created.



The following example describes how to create a template for FortiSwitch.
   a. Go to *FortiSwitch Manager* > *FortiSwitch Templates*.
   b. In the content pane, click *Create New*.
   c. Complete the options, and click *OK*.
   The template is created.

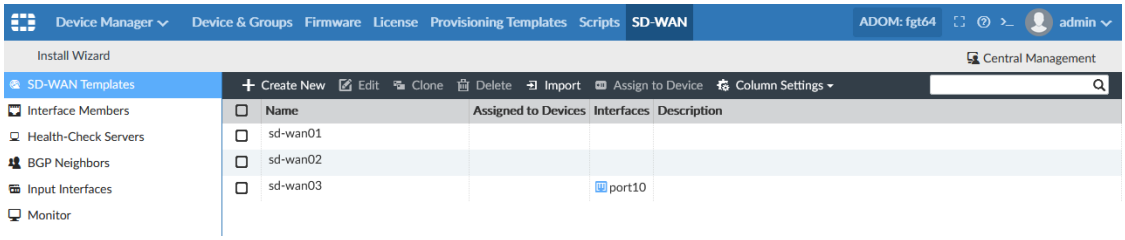


The following example describes how to create a template for SD-WAN.

a. Go to *Device Manager* > *SD-WAN* > *SD-WAN Templates*.

b. In the content pane, click *Create New*.

c. Complete the options, and click *OK*.
The template is created.



3. Create a new ADOM revision.
For example, name the revision *rev01*.

a. Go to *Policy & Objects*, and click *ADOM Revisions*.
The ADOM Revision dialog box is displayed.

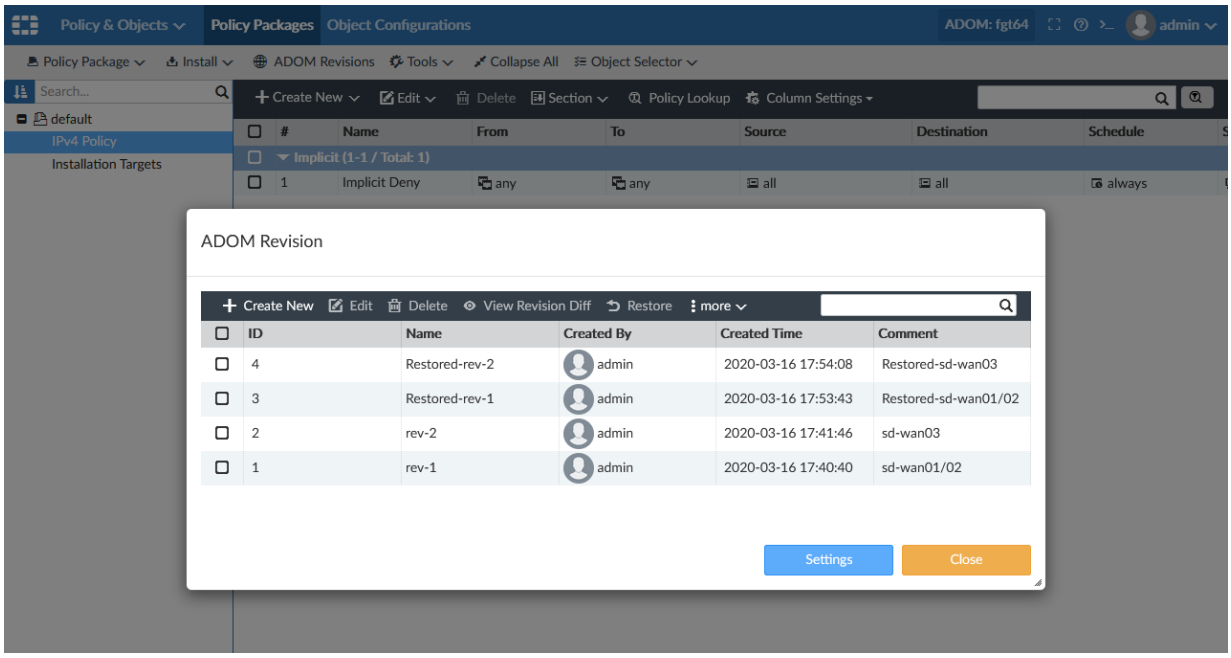
b. Click *Create New*.

c. Complete the options, and click *OK* to create the ADOM revision.

4. In the ADOM, modify any of the templates for FortiAP, SD-WAN, or FortiSwitch.

5. Create a new ADOM revision.
For example, name the revision *rev02*.

6. Restore ADOM revision *rev01*.
   a. Go to *Policy & Objects*, and click *ADOM Revisions*.
   b. Select the *rev01* revision, and click *Restore*.



7. Ensure that the templates from ADOM revision *rev01* are restored.
   In this example, check that the SD-WAN templates are restored.
   a. Go to *Device Manager* > *SD-WAN* > *SD-WAN Templates*.
   b. Review the templates.

FortiManager support for FortiGate-7000E and FortiCarrier-7000E families

FortiManager 6.4.0 supports the FortiGate-7000E and FortiCarrier-7000E families. Following is a list of supported FortiGate-7000E models:

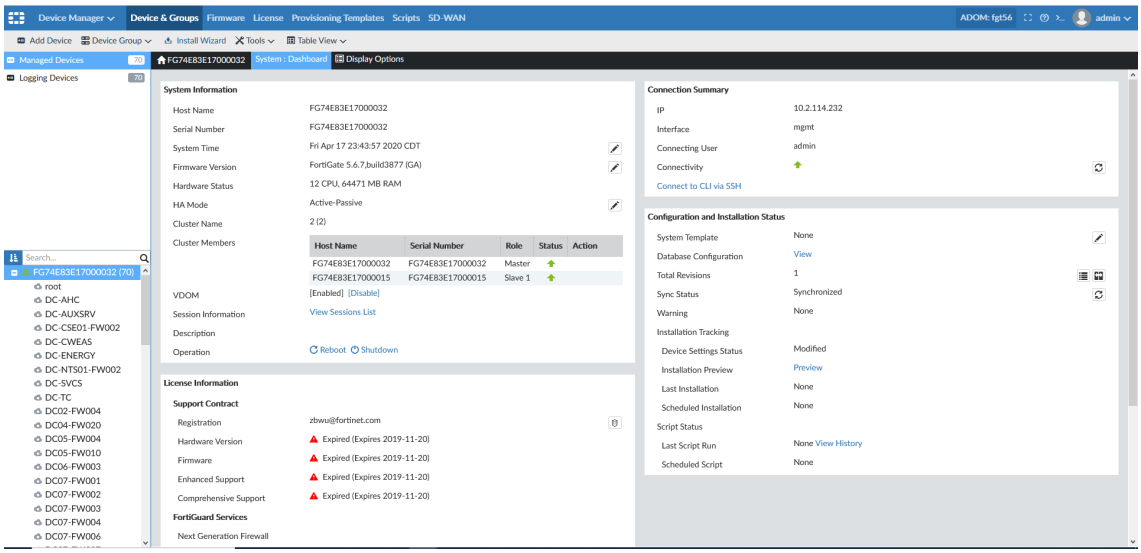
- FortiGate-7030E (FG73EQ)
- FortiGate-7030E (FG73ES)
- FortiGate-7040E (F74E8D)
- FortiGate-7040E (F74E9D)
- FortiGate-7040E (FG74E1)
- FortiGate-7040E (FG74E2)
- FortiGate-7040E (FG74E3)
- FortiGate-7040E (FG74E4)
- FortiGate-7040E (FG74E5)
- FortiGate-7040E (FG74E6)
- FortiGate-7040E (FG74E8)
- FortiGate-7040E (FG74E9)
- FortiGate-7060E (F76E9D)
- FortiGate-7060E (FG76E1)
- FortiGate-7060E (FG76E2)

- FortiGate-7060E (FG76E3)
- FortiGate-7060E (FG76E4)
- FortiGate-7060E (FG76E5)
- FortiGate-7060E (FG76E6)
- FortiGate-7060E (FG76E8)
- FortiGate-7060E (FG76E9)
- FortiGate-7060E-8-DC (F76E8D)

Following is a list of supported FortiCarrier-7000E models:

- FortiCarrier-7030E (FG73EQ)
- FortiCarrier-7030E (FG73ES)
- FortiCarrier-7040E (F74E8D)
- FortiCarrier-7040E (F74E9D)
- FortiCarrier-7040E (FG74E1)
- FortiCarrier-7040E (FG74E2)
- FortiCarrier-7040E (FG74E3)
- FortiCarrier-7040E (FG74E4)
- FortiCarrier-7040E (FG74E5)
- FortiCarrier-7040E (FG74E6)
- FortiCarrier-7040E (FG74E8)
- FortiCarrier-7040E (FG74E9)
- FortiCarrier-7060E (F76E9D)
- FortiCarrier-7060E (FG76E1)
- FortiCarrier-7060E (FG76E2)
- FortiCarrier-7060E (FG76E3)
- FortiCarrier-7060E (FG76E4)
- FortiCarrier-7060E (FG76E5)
- FortiCarrier-7060E (FG76E6)
- FortiCarrier-7060E (FG76E8)
- FortiCarrier-7060E (FG76E9)
- FortiCarrier-7060E-8-DC (F76E8D)

The following example shows *Device Manager* for the FortiGate-7040E:



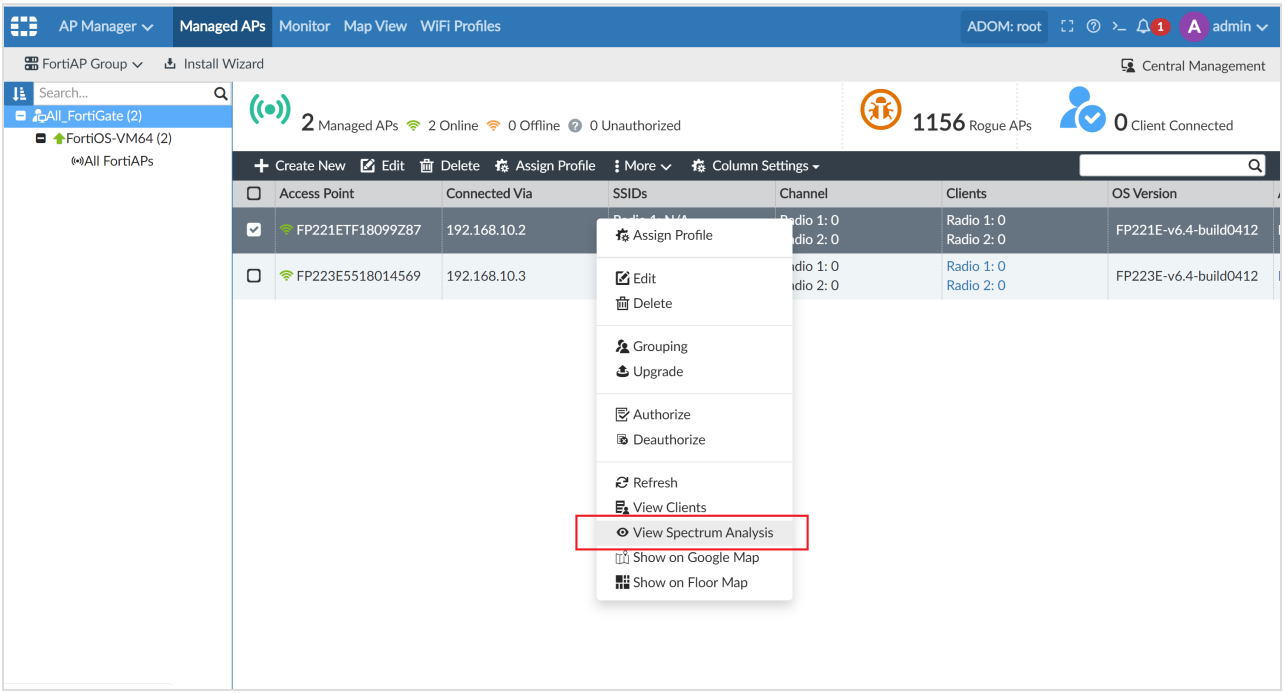
Spectrum analysis for managed APs - 6.4.1

You can view the spectrum analysis for managed APs in FortiManager 6.4. Spectrum analysis is available through *AP Manager > Managed APs*.

To view the spectrum analysis for a managed AP in the FortiManager GUI:

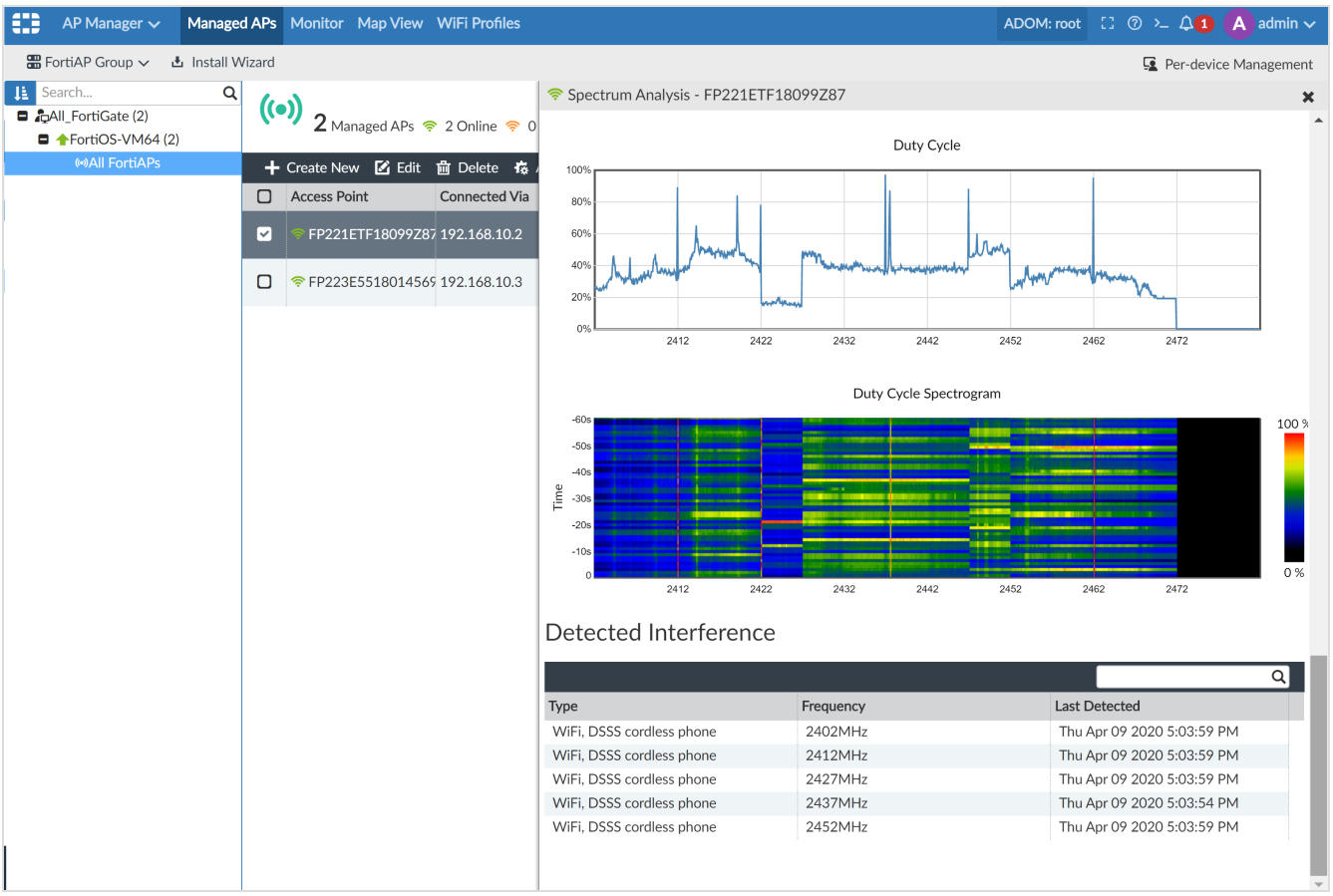
1. Ensure the *JSON API Access* field is set to *Read-Write*, by editing the administrator. See *Editing administrators* in the *FortiManager Administration Guide*.
2. Create a new WiFi profile or modify an existing WiFi profile, by setting the radio mode setting to *Dedicated Monitor*. See *AP profiles* in the *FortiManager Administration Guide*.
3. Assign the profile to the managed AP. See *Assigning profiles to FortiAP devices* in the *FortiManager Administration Guide*.
4. Use the *Install Wizard* to install the changes to FortiGate. See *Using the Install Wizard to install device settings only* in the *FortiManager Administration Guide*.

5. On the *Managed APs* screen, select a managed AP, click *More* from the toolbar or right-click, and click *View Spectrum Analysis*:



The *Spectrum Analysis* in the form of *Signal Interference*, *Signal Interference Spectrogram*, *Duty Cycle*, and *Duty Cycle Spectrogram* charts, along with the tabulated *Detected Interference* information is displayed.


AP Manager
Managed APs
Monitor
Map View
WiFi Profiles
ADOM: root
admin
FortiAP Group
Install Wizard
Central Management
Search...
All_FortiGate (2)
FortiOS-VM64 (2)
All FortiAPs
2 Managed APs
2 Online
0 Offline
0 Unauth
Create New
Edit
Delete
Assign Profile
Access Point
Connected Via
FP221ETF18099Z87
192.168.10.2
FP223E5518014569
192.168.10.3
Spectrum Analysis - FP221ETF18099Z87
AP capabilities will be limited during spectrum analysis.
Band
2.4 GHz
5 GHz
Channels
1-13
X-Axis
Mhz
Channels
Stop
Restart
Analysis
Signal Interference
dBm
Persistent
Transient
Signal Interference Spectrogram
Time
-20 dBm
-100 dBm



AP capabilities will be limited during spectrum analysis.

FortiSwitch GUI enhancements - 6.4.1

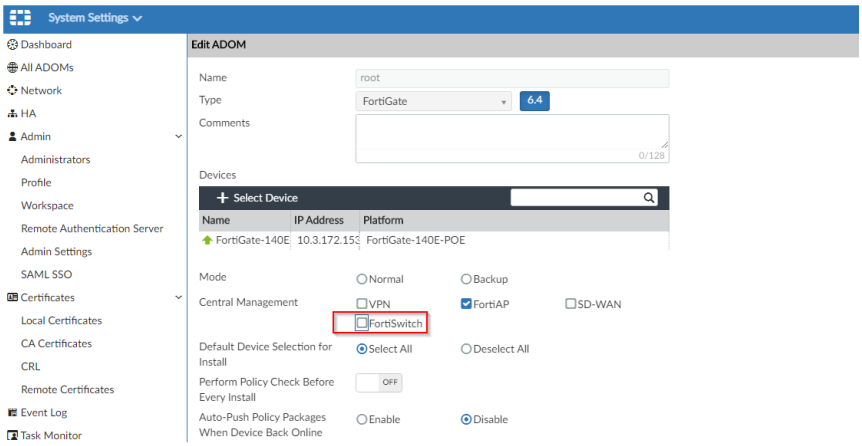
FortiManager includes the following GUI enhancements for FortiSwitch Manager:

- NAC policy
- ports table
- connected device
- transceiver information

These features are only available in per-device FortiSwitch Management mode.

To enable FortiSwitch per-device management:

1. Go to System *Settings* > *All ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, clear the *FortiSwitch* checkbox, and click *OK*.



Central management is disabled, and per-device management is enabled for FortiSwitch.

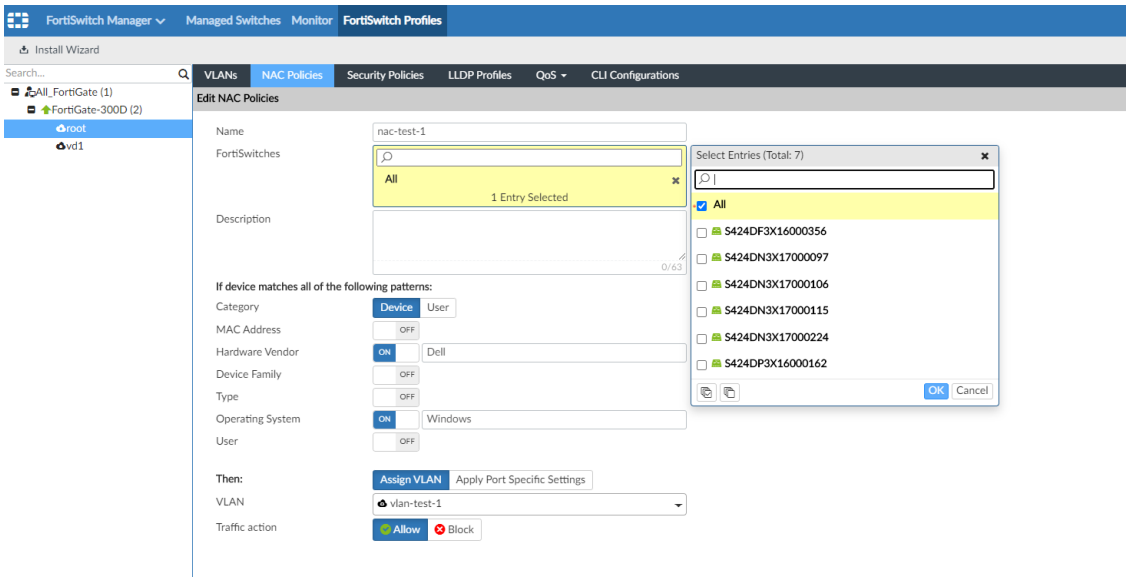
4. Go to *FortiSwitch Manager*, and notice that *Per-device Management* is displayed in the top-right corner.

NAC Policy

NAC policies can be created or edited in *FortiSwitch Profile* > *NAC Policies*. Once the policies are created or editied, the changes can be installed to the FortiGate.

To edit NAC policies:

1. Go to *FortiSwitch Manager* > *FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.
   The *VLANs* tab is displayed.
3. Click the *NAC Policies* tab.
   The NAC policies are displayed.
4. Right-click the NAC policy and select *Edit*.
   The *Edit NAC Policies* pane opens.



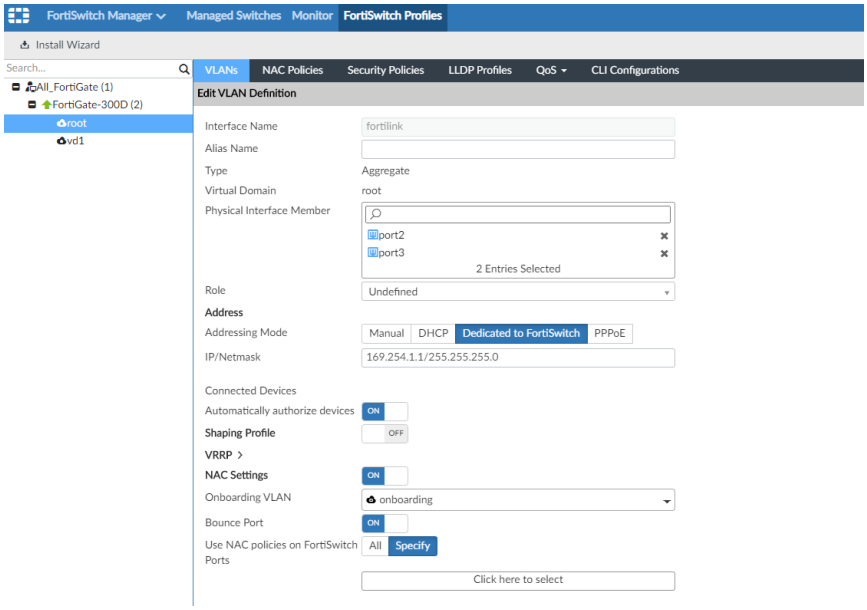
5. Edit your NAC policy, and click *OK*.
   The changes are saved to the FortiGate database.

NAC Settings in FortiLink Interface

You can edit NAC settings via the FortiLink interface.

To edit NAC settings via the FortiLink interface:

1. Go to *FortiSwitch Manager > FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.
   The *VLANs* tab is displayed.
3. In *FortiLink Interface* pane, select a FortiLink and click *Edit* or right-click the FortiLink and select *Edit*.
   The *Edit VLAN Definition* pane opens.

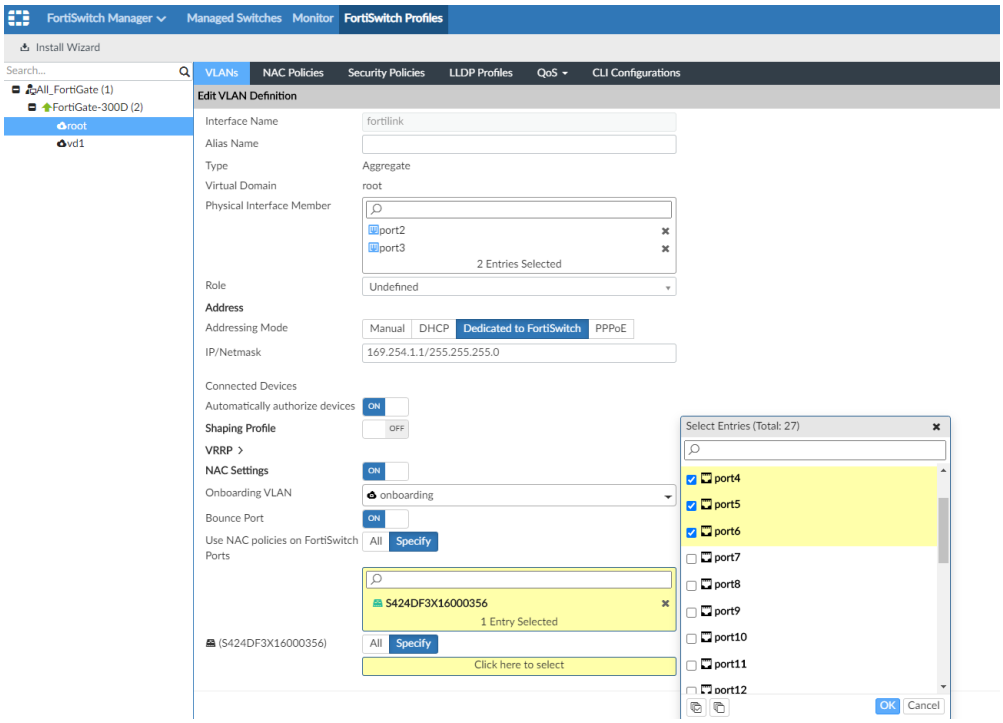


By default, *NAC Settings* option is enabled and *Onboarding VLAN* is set to *onboarding*. You may disable the *NAC Settings* or change the onboarding VLAN.

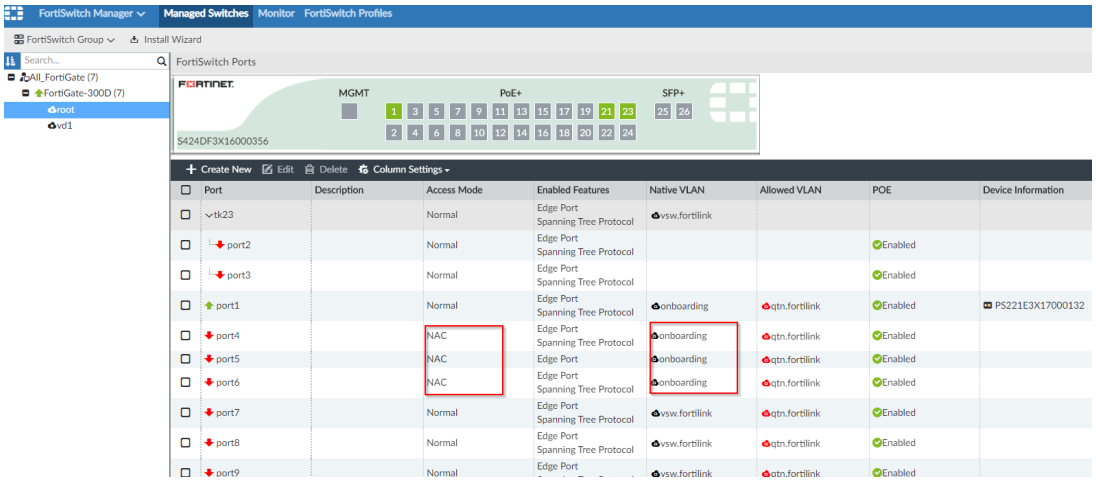
4. In the *Edit VLAN Definition* pane, set *Use NAC policies on FortiSwitch Ports* to *Specify*.
5. Select *Click here to select* and from the *Select Entries* list, select the FortiSwitch. Click *OK*.

If you want to specify NAC policies on all FortiSwitches, set *Use NAC policies on FortiSwitch Ports* to *All*.

6. In the FortiSwitch option below *Use NAC policies on FortiSwitch Ports*, select *Specify*.
7. Select *Click here to select* and from the *Select Entries* list, select the ports to specify the NAC policy on. Click *OK*. Click *OK* to save your changes.



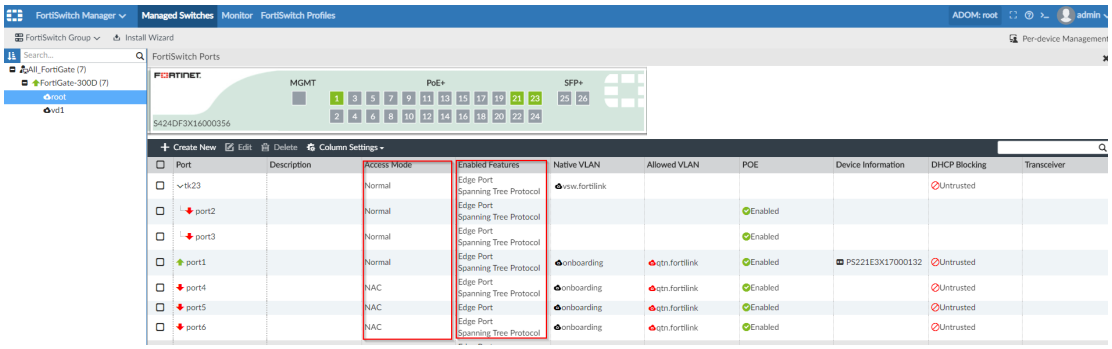
8. Go to *Managed Switches*, and double-click the previously specified FortiSwitch. The *FortiSwitch Ports* pane opens.



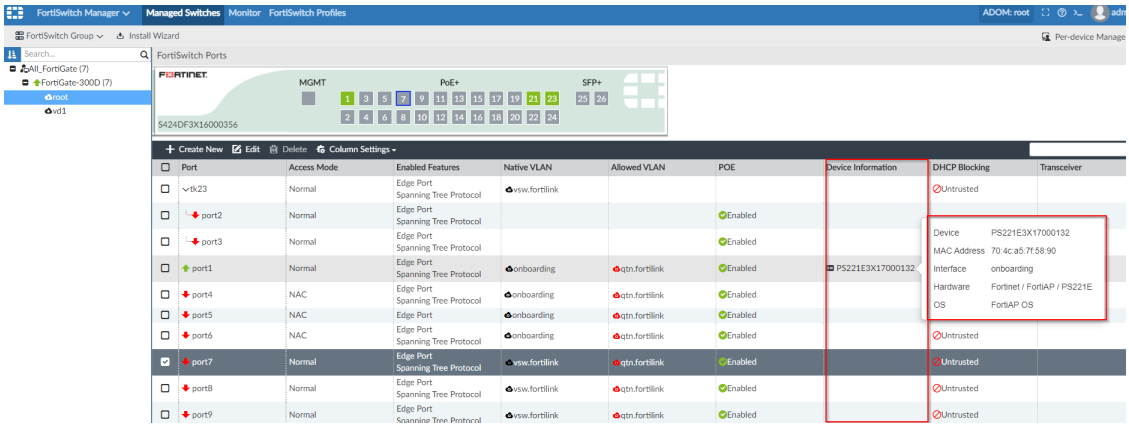
NAC policy is enforced on the selected ports.

FortiSwitch Ports table GUI enhancements

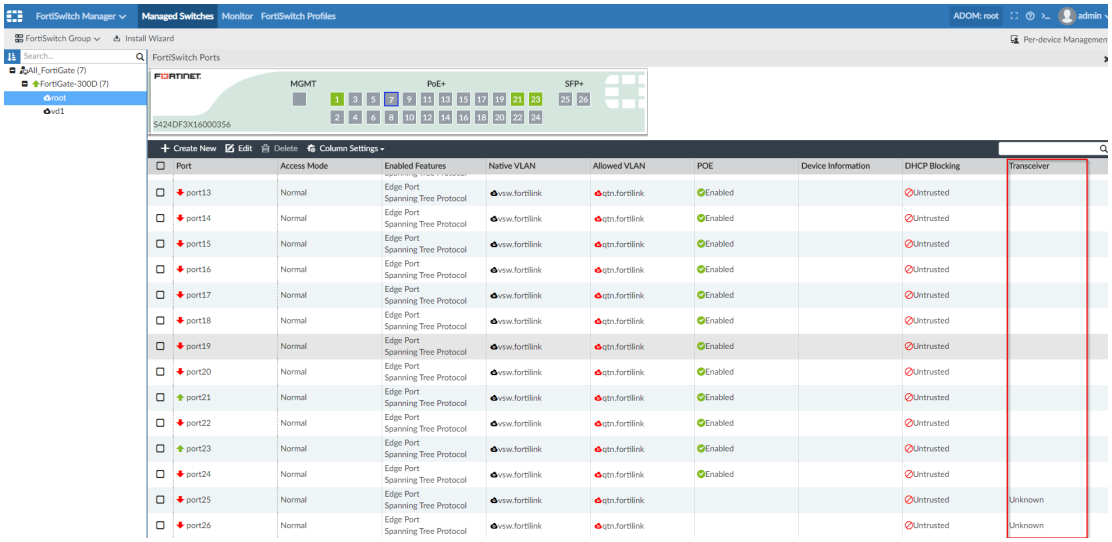
1. Go to FortiSwitch *Manager* > *Managed Switches*.
2. In the tree menu, select a FortiGate.
   The list of managed switches is displayed in the content pane.
3. Double-click a switch.
   The *FortiSwitch Ports* pane opens.
   The *Access mode* column is added to show the port access mode: *NAC* or *Normal*.
   The *Enabled Features* column is added to show if *Edge Port* or *Spanning Tree Protocol* is enabled.



The *Device Information* column is added to show the connected device information.
Hover over the listed device to see detailed information.

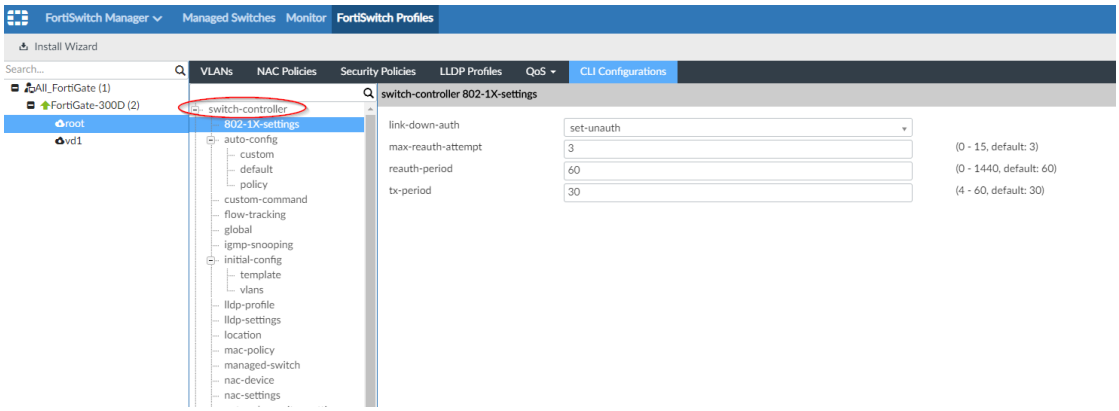


The *Transceiver* column is added to display transceiver information. If no transceiver is connected, then the *Transceiver* column shows *Unknown*.



FortiSwitch CLI Configuration

1. Go to *FortiSwitch Manager* > *FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.
   The *VLANs* tab is displayed.
3. Click the *CLI Configurations* tab.
   The *CLI Configurations* tab opens.



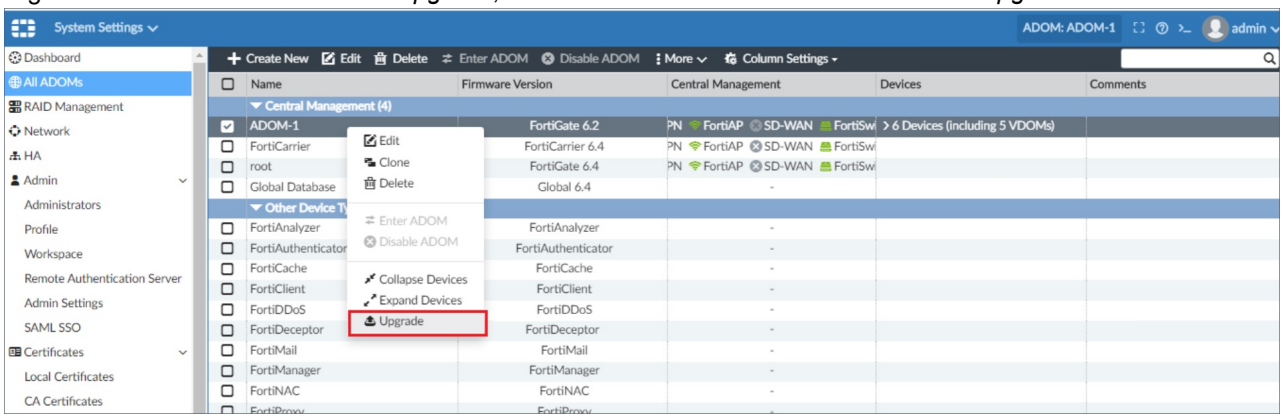
The *CLI Configurations* tab is added to edit and display all the settings for the switch-controller.

Upgrading ADOMs managing devices running FortiOS 6.4 - 6.4.1

ADOMs can concurrently manage devices running FortiOS 6.2 and 6.4. After all the devices being managed by an ADOM are upgraded to FortiOS 6.4, you can upgrade the ADOM.

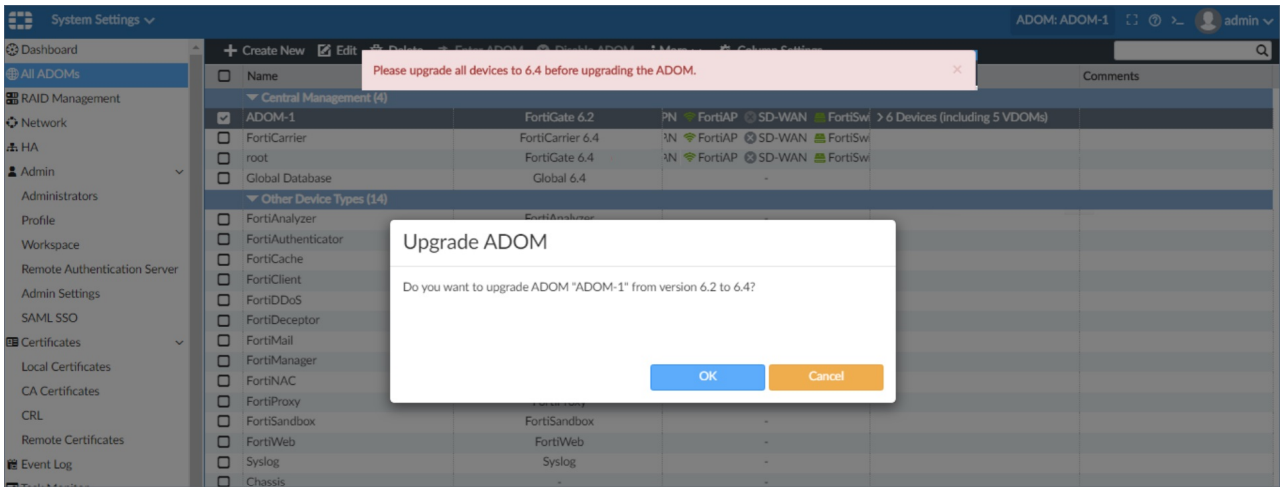
To upgrade an ADOM:

1. Go to *System Settings* > *All ADOMs*.
2. Right-click on an ADOM and select *Upgrade*, or select an ADOM and then select *More* > *Upgrade* from the toolbar.



If the ADOM has already been upgraded to the latest version, this option will not be available.

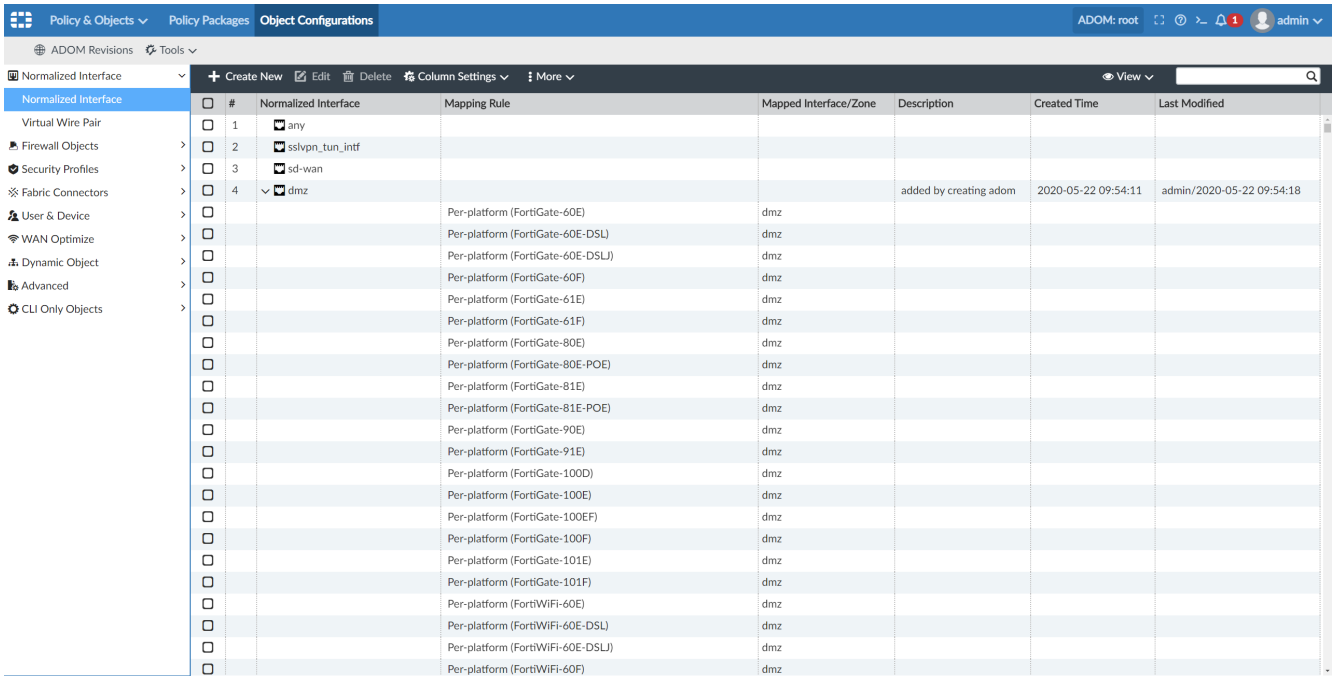
3. Select *OK* in the confirmation dialog box to upgrade the device.
If all of the devices within the ADOM are not already upgraded, the upgrade will be aborted and an error message will be shown.



Upgrade the remaining devices within the ADOM, then return to step 1 to try upgrading the ADOM again.

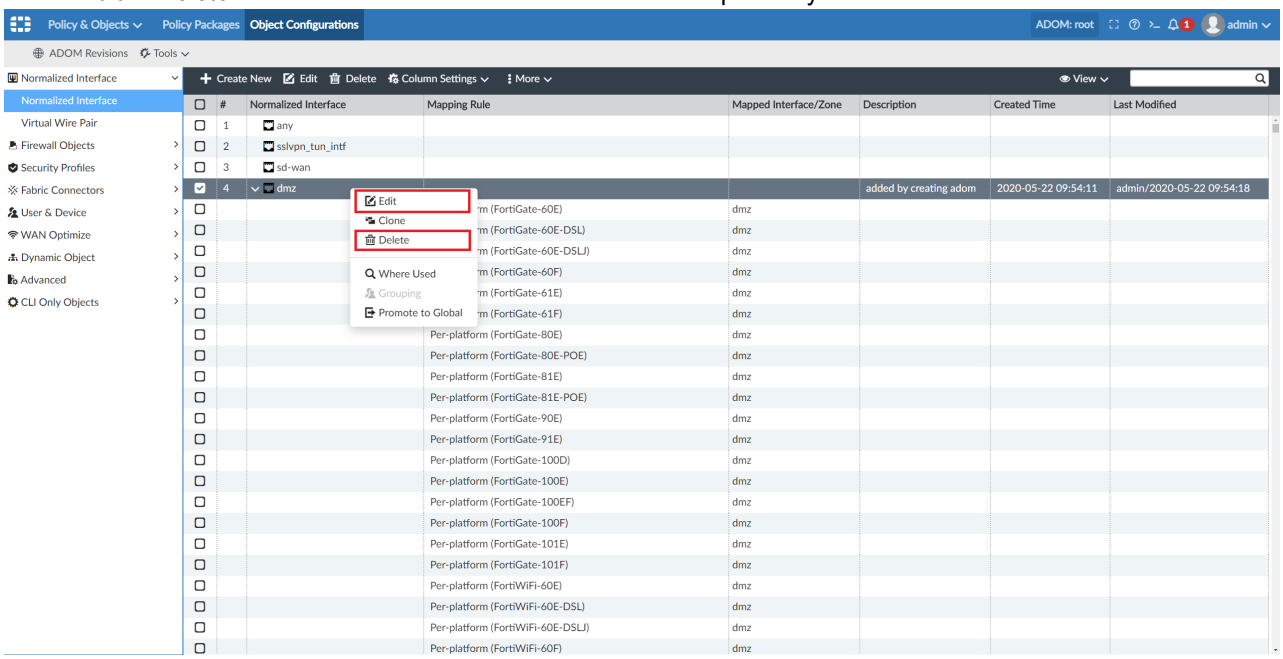
Interface normalization policy - 6.4.1

When an ADOM is created, a number of per-platform interfaces are defined for all FortiGate models by default. This allows all FortiGate models to have a number of normalized interfaces already mapped, so that policies can be installed without custom mapping. The interface names could be matched to different real interfaces on different FortiGate models. All mappings are explicitly shown in the mapping table. If there is no match, mapping will not exist.



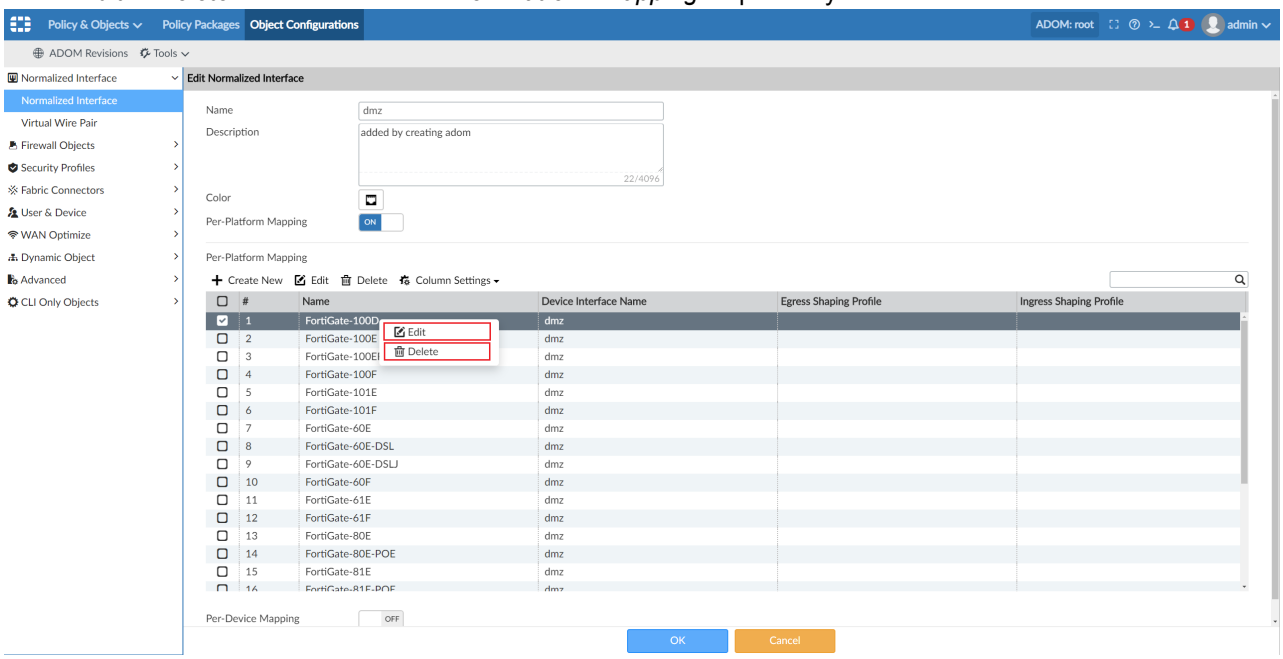
A normalized interface can be edited or deleted. To edit or delete a normalized interface:

1. Right-click on a normalized interface entry in the *Normalized Interface* table.
2. Select *Edit* or *Delete* to edit or delete the normalized interface respectively.



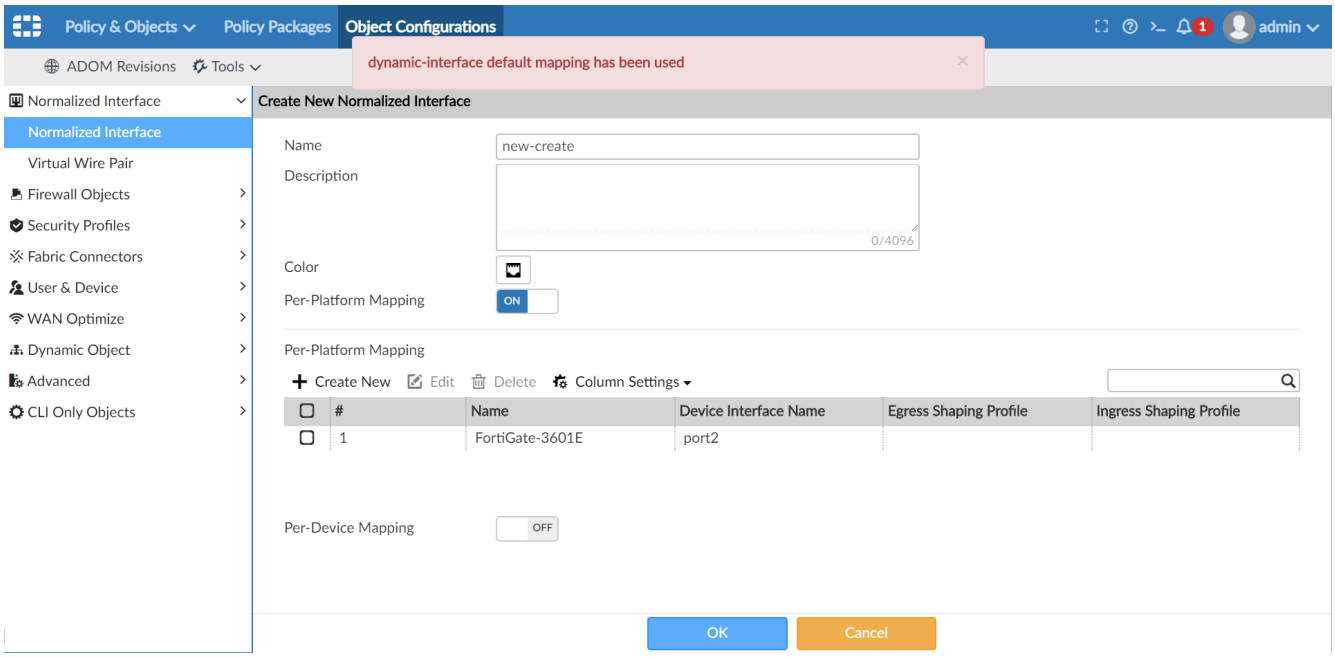
The *Per-Platform Mapping* in a normalized interface can be edited or deleted. To edit or delete the *Per-Platform Mapping* in a normalized interface:

1. Right-click on a normalized interface entry in the *Normalized Interface* table.
2. Select *Edit*. The *Edit Normalized Interface* page appears.
3. In the *Per-Platform Mapping* table, right-click on a table entry.
4. Select *Edit* or *Delete* to edit or delete the *Per-Platform Mapping* respectively.

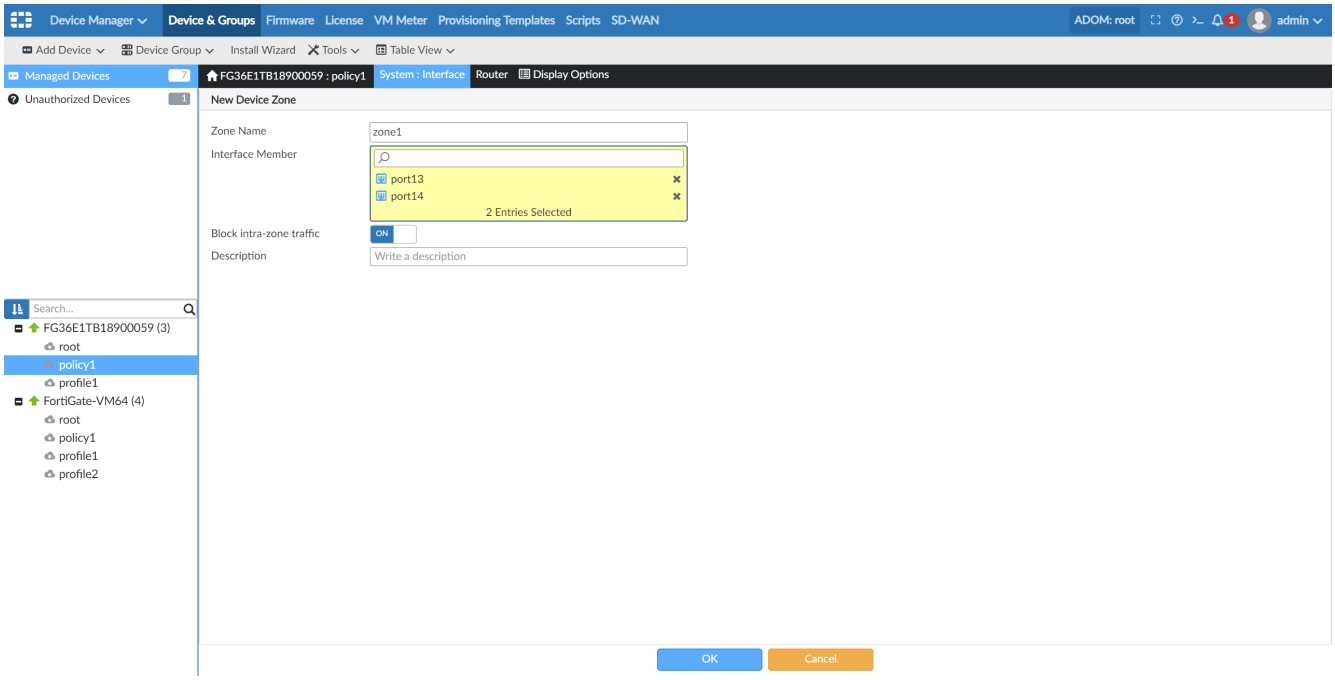


A normalized interface may use *Per-Platform* mapping and/or *Per-Device* mapping. In a policy, a per-device mapping has a higher priority than a per-platform mapping.

When creating a new normalized interface, to use a physical interface name in the per-platform mapping, the default per-platform mapping should be deleted from the default per-platform interface first. Otherwise the system will throw an error and the interface cannot be created.



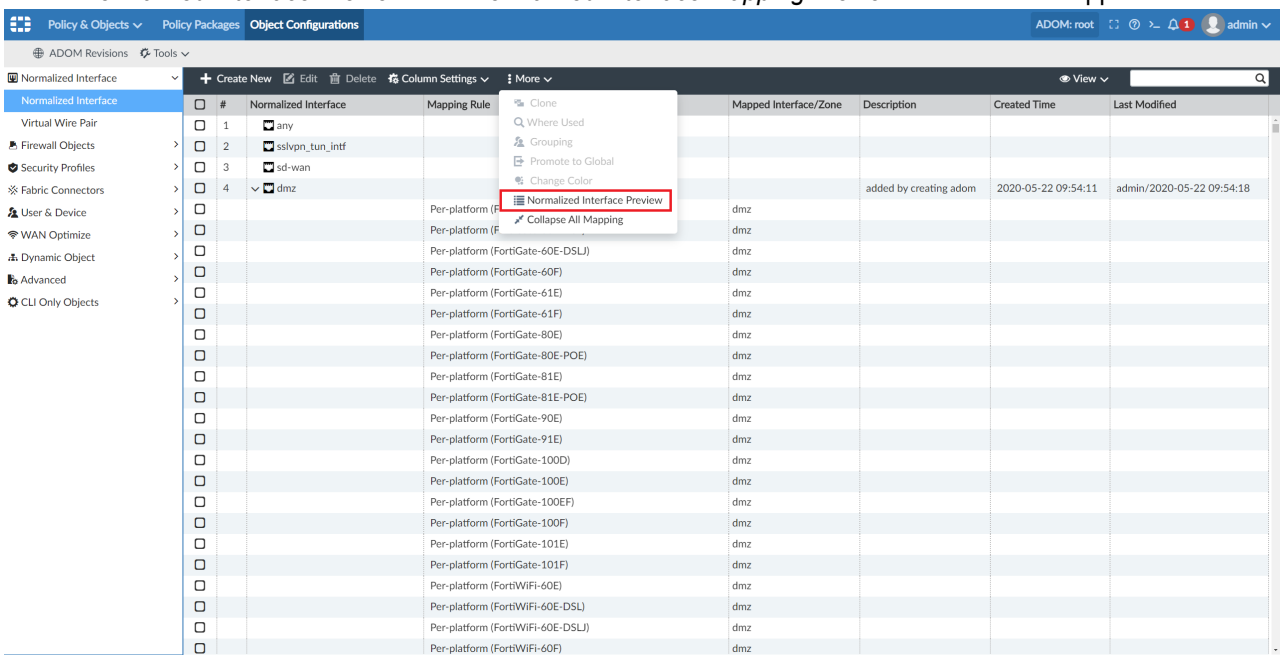
When creating a zone, map it to a normalized interface just like mapping to a regular interface.



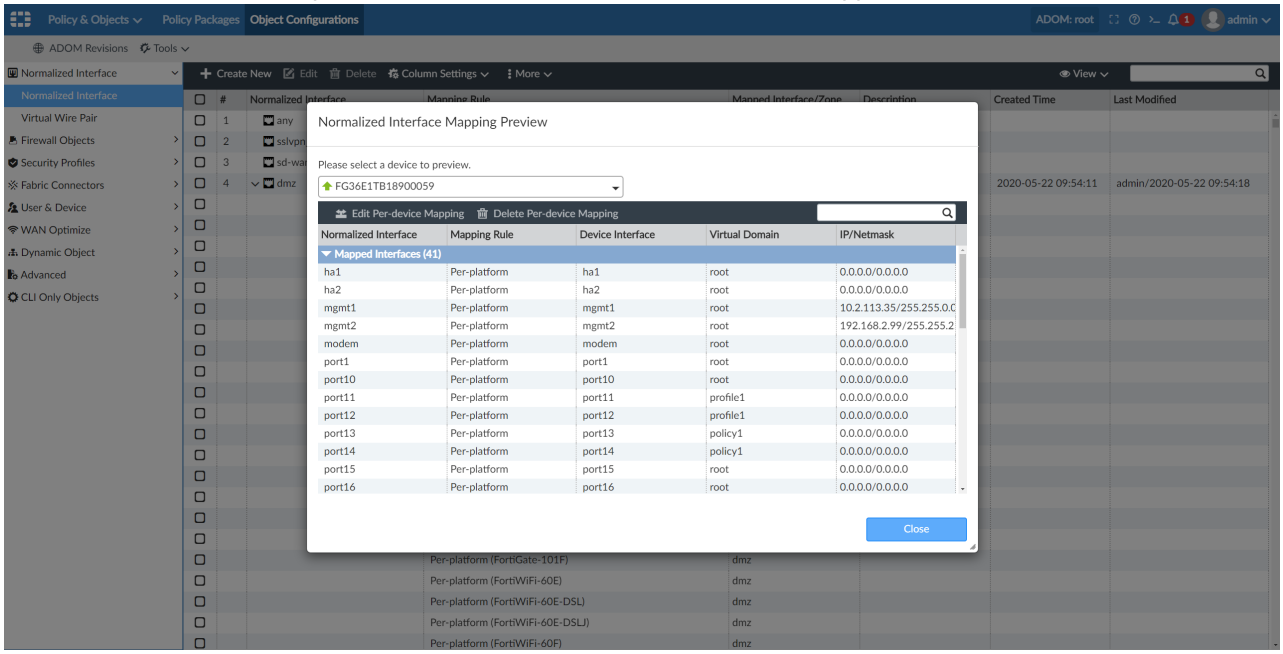
For each managed FortiGate device you can view the number of normalized interfaces mapped to it. To view the normalized interfaces mapped to a FortiGate:

1. Select a normalized interface from the *Normalized Interface* table.
2. Click *More* from the toolbar above the table. A drop-down menu drops down.

3. Select *Normalized Interface Preview*. The *Normalized Interface Mapping Preview* modal window appears.

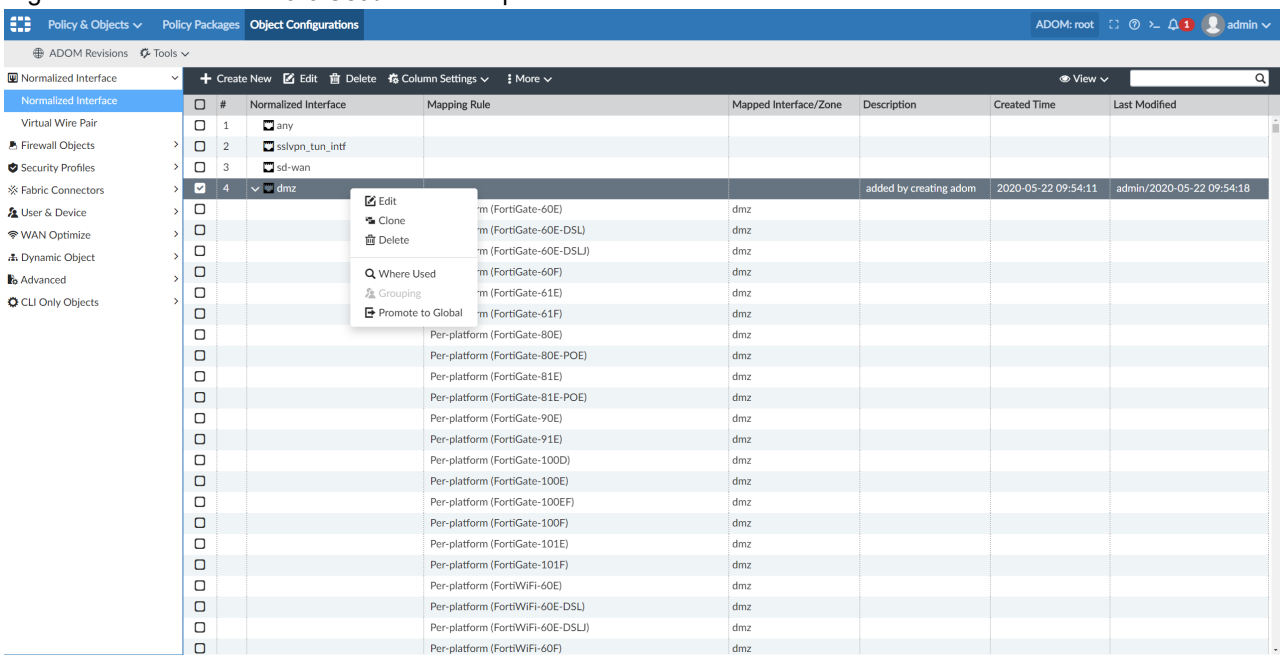


4. Select a device from the drop-down list to view the normalized interfaces mapped to it.

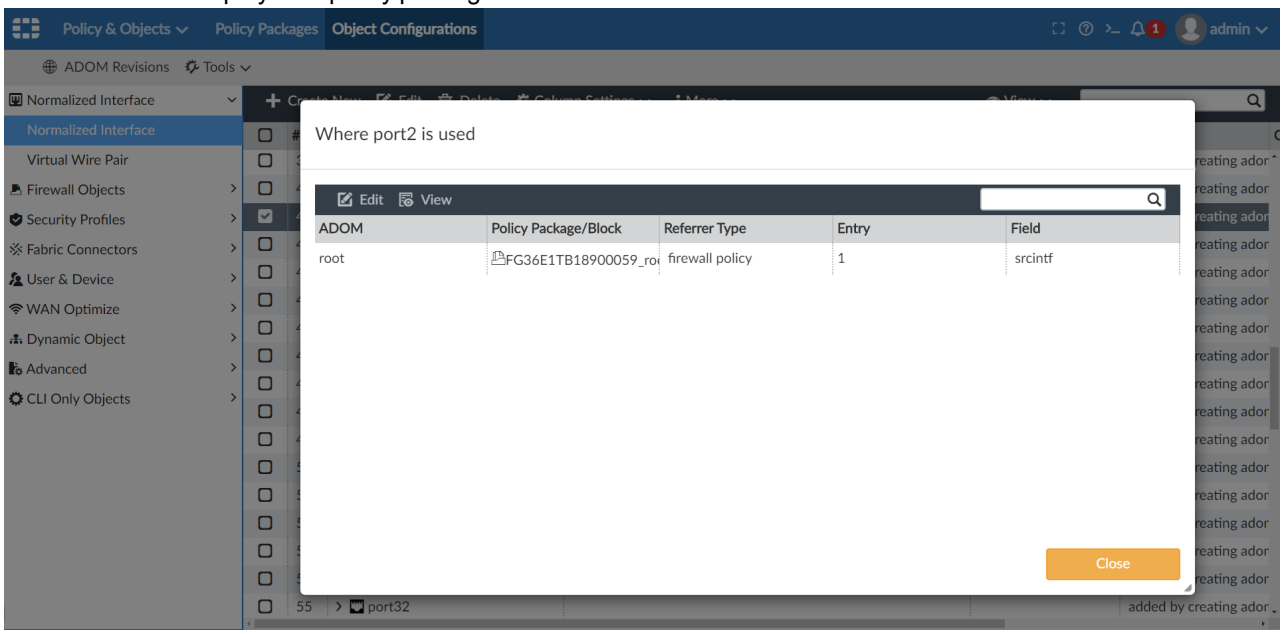


You can search for where a normalized interface is configured in a policy package. To search for where a normalized interface is used in a policy package:

1. Select a normalized interface from the *Normalized Interface* table.
2. Right-click and select *Where Used* from the options.

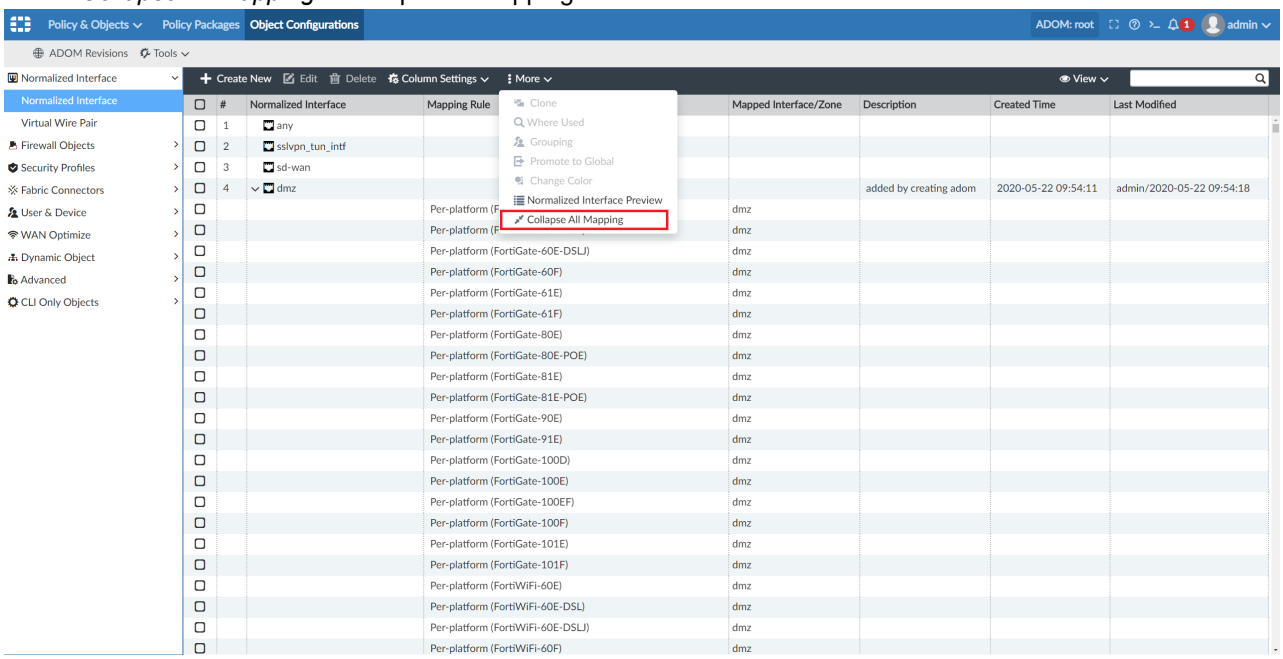


3. A modal window displays the policy package which the selected normalized interface is used in.

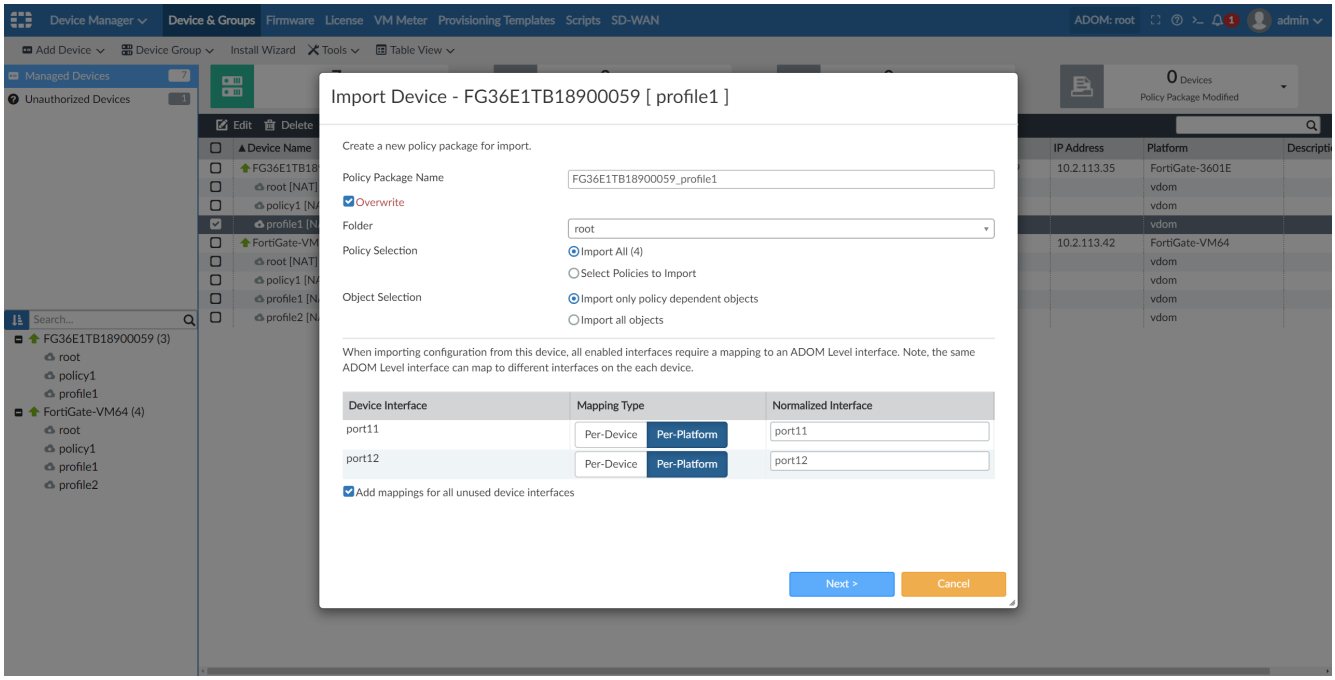


You may collapse or expand all the mappings in the *Normalized Interface* table. To collapse or expand all mappings:

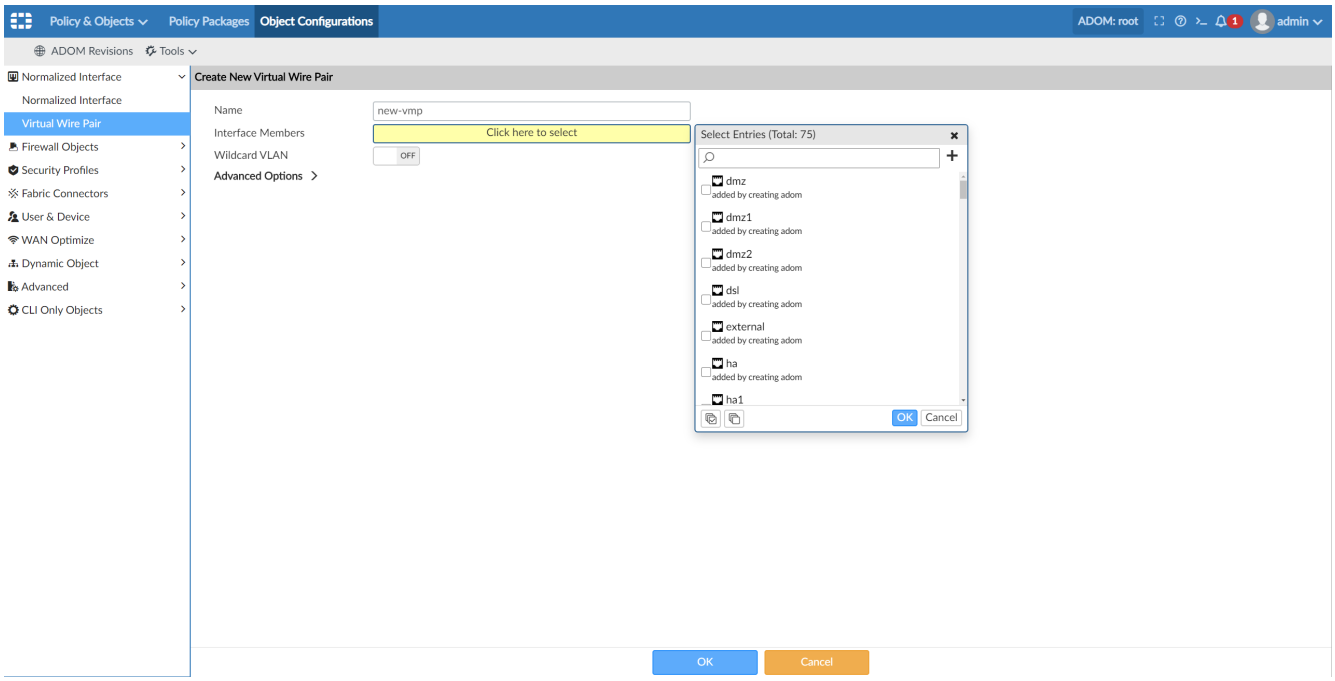
1. Click *More* from the toolbar above the *Normalized Interface* table.
2. Select *Collapse All Mapping* to collapse all mappings.



When importing a device, you can choose the mapping type of the device interface to be either *Per-Platform* or *Per-Device*.



You can use normalized interfaces as *Virtual Wire Pair* members.

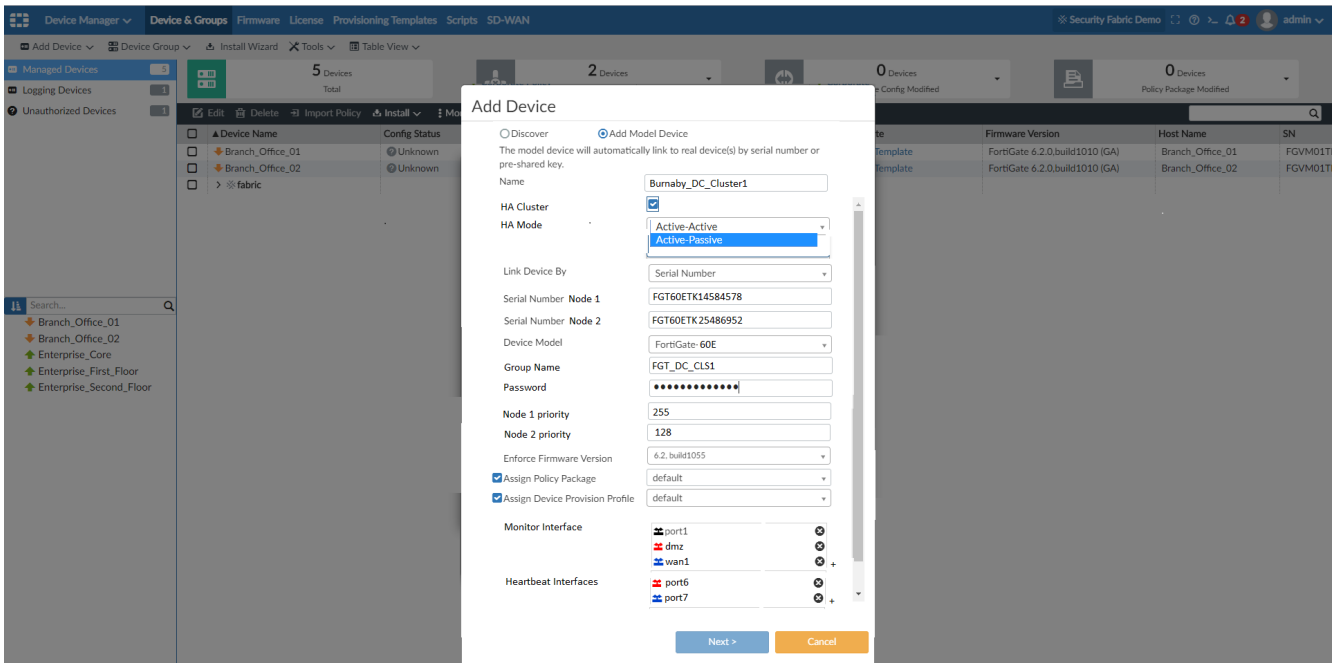


Adding a FortiGate HA cluster when adding a model device - 6.4.1

You can add a FortiGate HA cluster using the *Add Model Device* method when adding a new device. The process of adding a FortiGate HA cluster is similar to adding a model device using FortiGate serial numbers. See *Adding a model device by serial number* in the *FortiManager Administration Guide*.

You can add the two FortiGate devices as model devices to be part of the HA cluster. In the *Add Device* dialog, select *Add Model Device*, and select the *HA Cluster* option. Populate the mandatory fields *HA Mode*, *Serial Number* for both the nodes, *Device Model* type, *Group Name* and *Password* for the HA cluster, *Node 1* and *Node 2* priority, *Monitor*

Interface members, and *Heartbeat Interface* members.



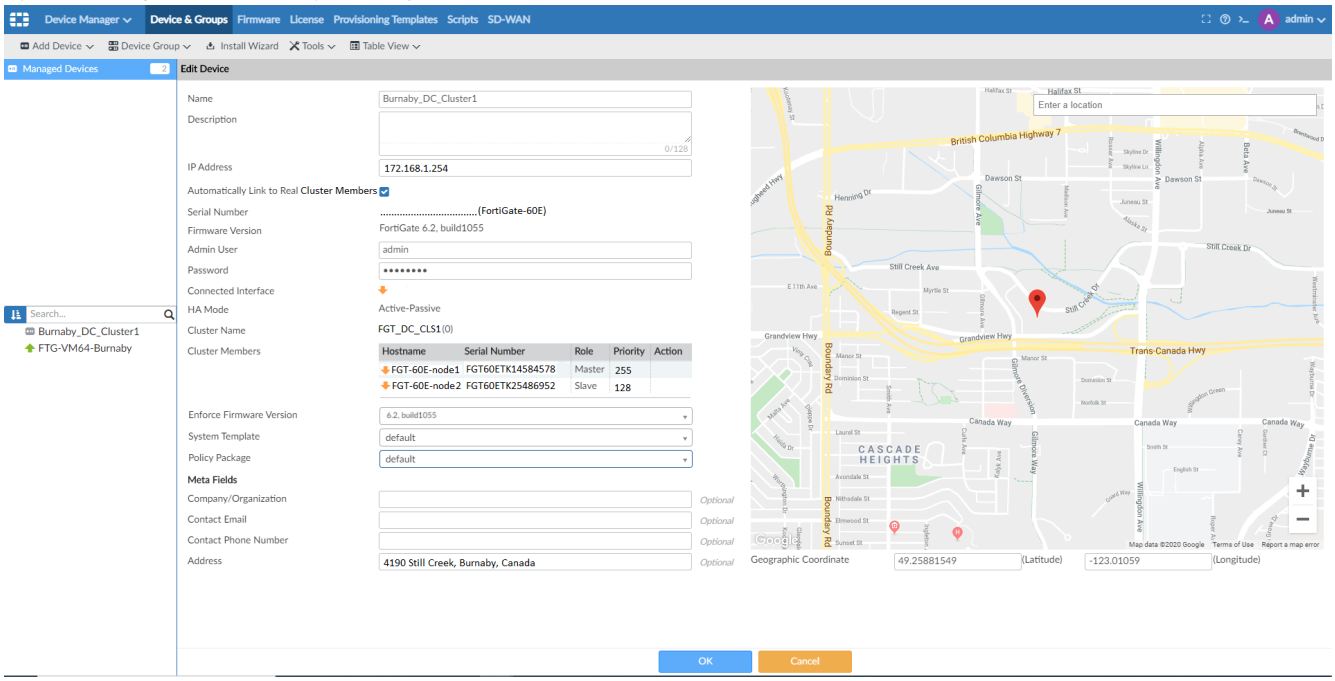
The FortiGate device with a higher node priority will be considered as the primary device of the HA cluster.

Both the FortiGate devices to be added to the HA cluster must be on the same firmware version. If not, the devices will be enforced with the same version as selected in the *Enforce Firmware Version* field in the *Add Device* dialog.

FortiManager adds both the FortiGate devices as model devices and creates an HA cluster. Based on device node priorities, both the devices will come online and show up in FortiManager one after the other. You can view the status of the HA cluster and information about each of the nodes of the HA cluster in *Device Manager*.

You can also edit the HA cluster information after adding it. Use the *Edit Device* screen to modify the HA cluster information by modifying the fields *IP Address*, *Admin User* and *Password*, *Cluster Members*, *Enforce Firmware Version*,

System Template, and *Policy Package*.



Updated Security Rating Report - 6.4.1

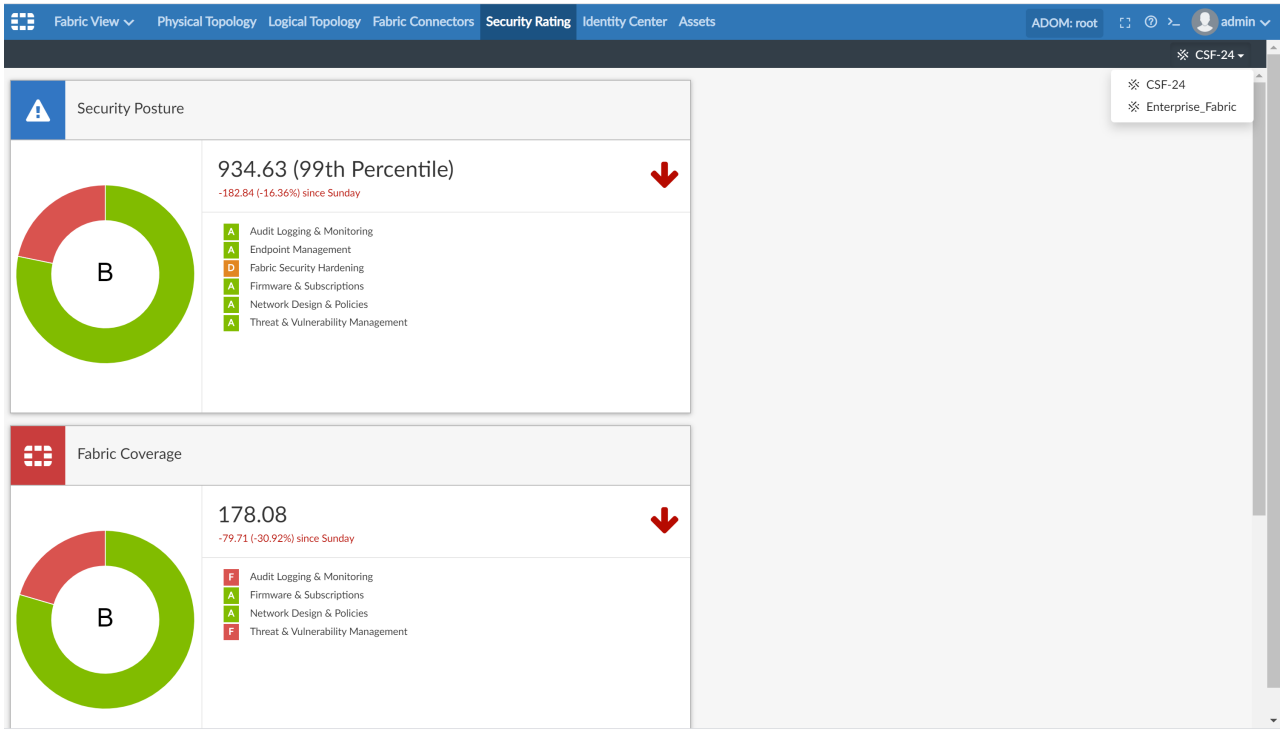
The Security Rating report in FortiManager has been synched with the FOS v6.4 version of the report. The FortiManager Security Rating report now has the same style and content as the FortiGate 6.4 version of the report.

Requirements:

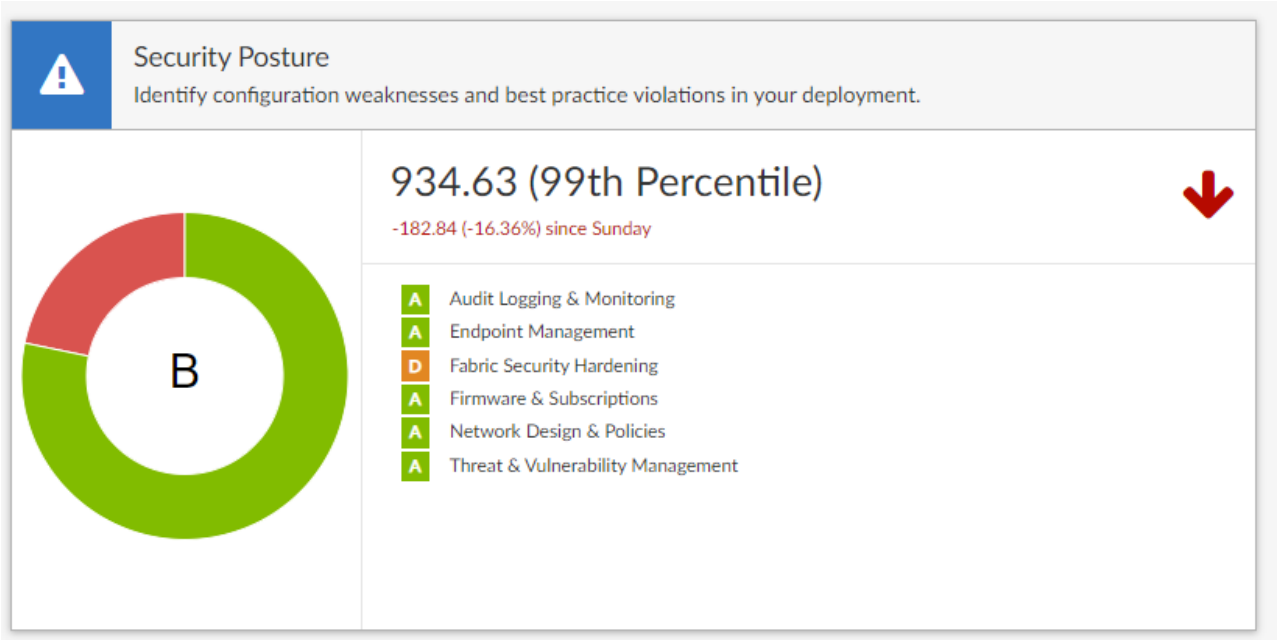
Use FortiOS to generate the Security Fabric Ratings report to view the information in FortiManager.

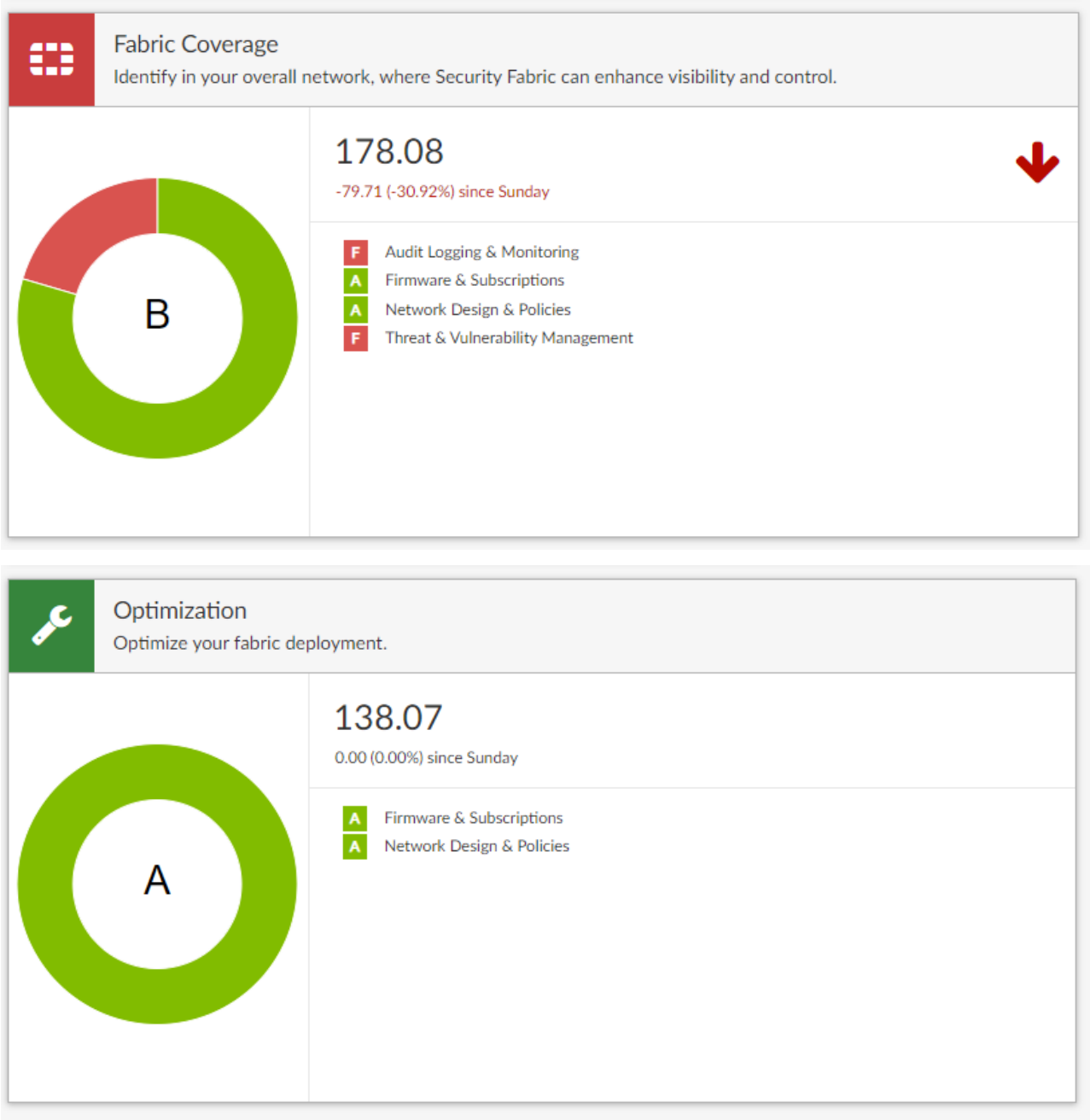
To view the Security Rating report:

1. Go to *Fabric View* > *Security Rating*.
   The Security Rating pane displays Security Fabric Ratings of configurations for FortiGate Security Fabric groups. You can view the results for multiple FortiGate Security Fabric groups.

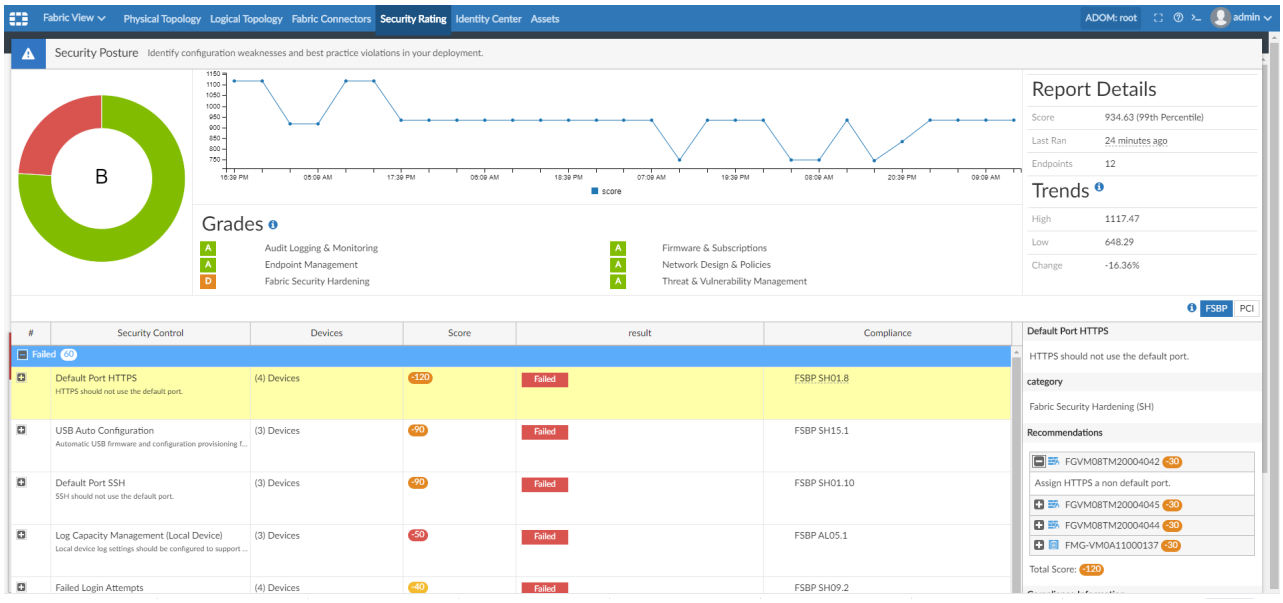


The Security Rating pane is separated into three major scorecards: *Security Posture*, *Fabric Coverage*, and *Optimization*, which provide an executive summary of the three largest areas of security focus in the Security Fabric.





2. Click a scorecard to view the drilldown report with itemized results and compliance recommendations.
The point score represents the net score for all passed and failed items in that area. The report includes the security controls that were tested against, linking to specific FSBP or PCI compliance policies.

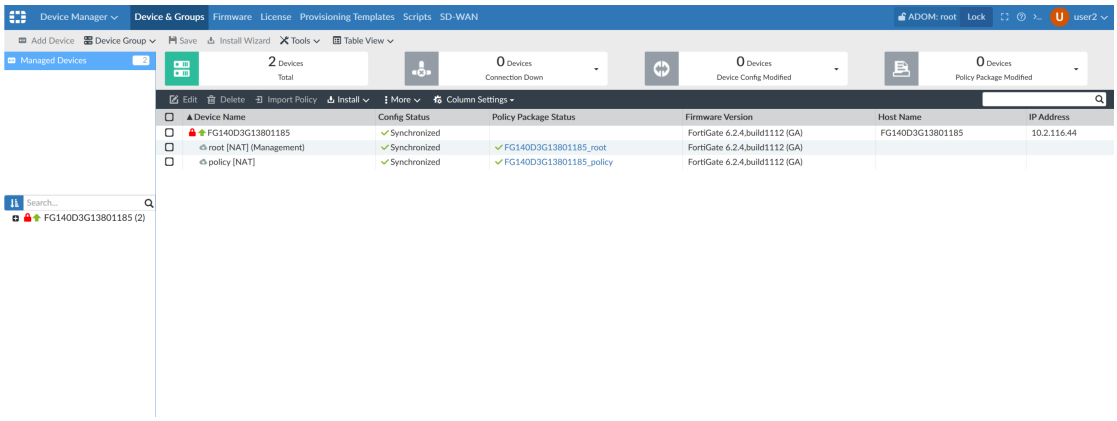


3. To exit the current view, click the icon beside the scorecard title to return to the summary view.

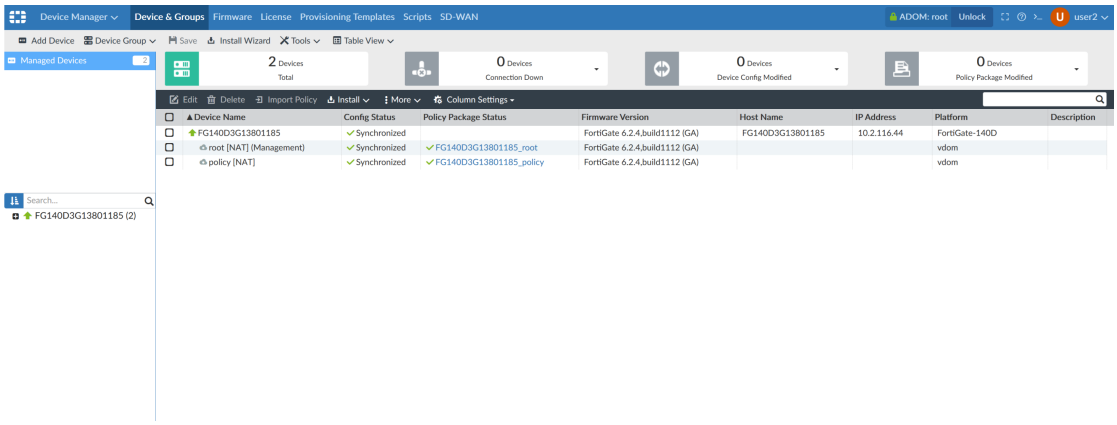
ADOM locking for FortiGates with multiple VDOMs used in multiple ADOMs - 6.4.1

A FortiGate can have multiple VDOMs. In advanced ADOM mode in FortiManager, you can assign VDOMs of a FortiGate to different ADOMs. If a user locks an ADOM and installs configurations to one of the VDOMs, other users can lock other ADOMs that have VDOMs for the FortiGate.

For example, FortiManager has advanced ADOM mode enabled, and there are two users: user1 and user2. A FortiGate has VDOMs that are assigned to the root ADOM and a test ADOM. In the test ADOM, the first user (user1) locks the ADOM, and installs a configuration to a VDOM of the FortiGate. In the root ADOM, the second user (user2) can view the red lock icon, for example:



The second user can lock the root ADOM. The following example, shows the locked root ADOM:

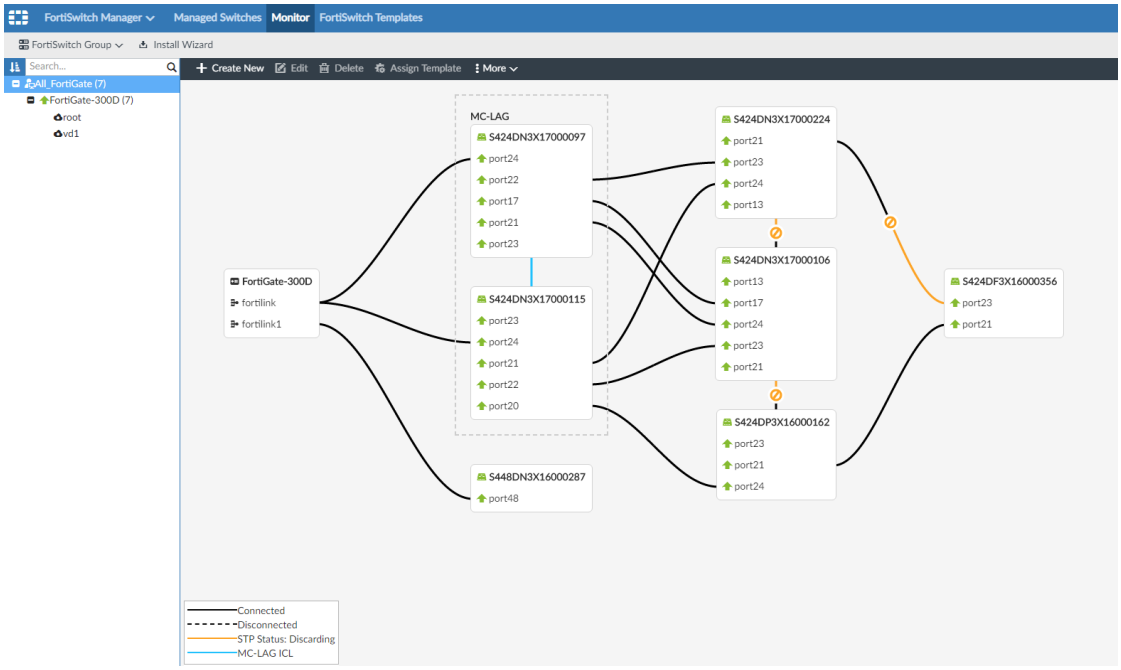


New and improved FortiSwitch Topology View - 6.4.2

You can now see topology view similar to FortiOS for selected devices. This gives you the visibility of the managed FortiSwitch status, connection topology, and MC-LAG status among others.

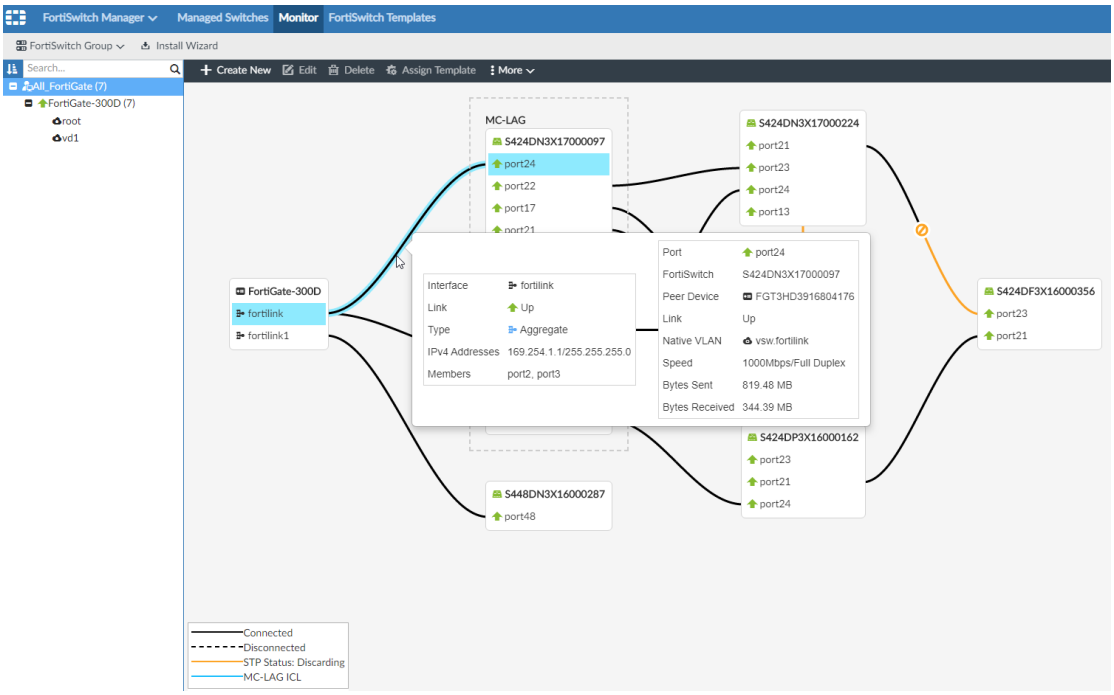
To view the FortiSwitch topology:

1. Go to *FortiSwitch Manager* > *Monitor*.
2. In the tree menu, select the FortiGate.
   The FortiSwitch connection topology is displayed.

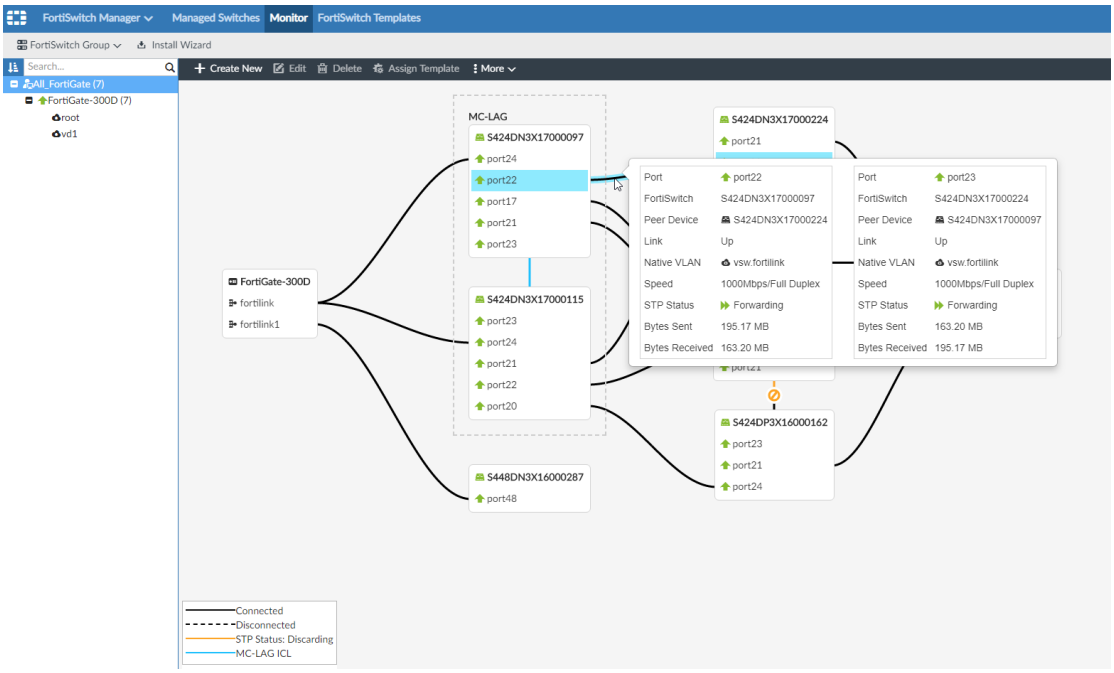


To view the FortiSwitch topology information:

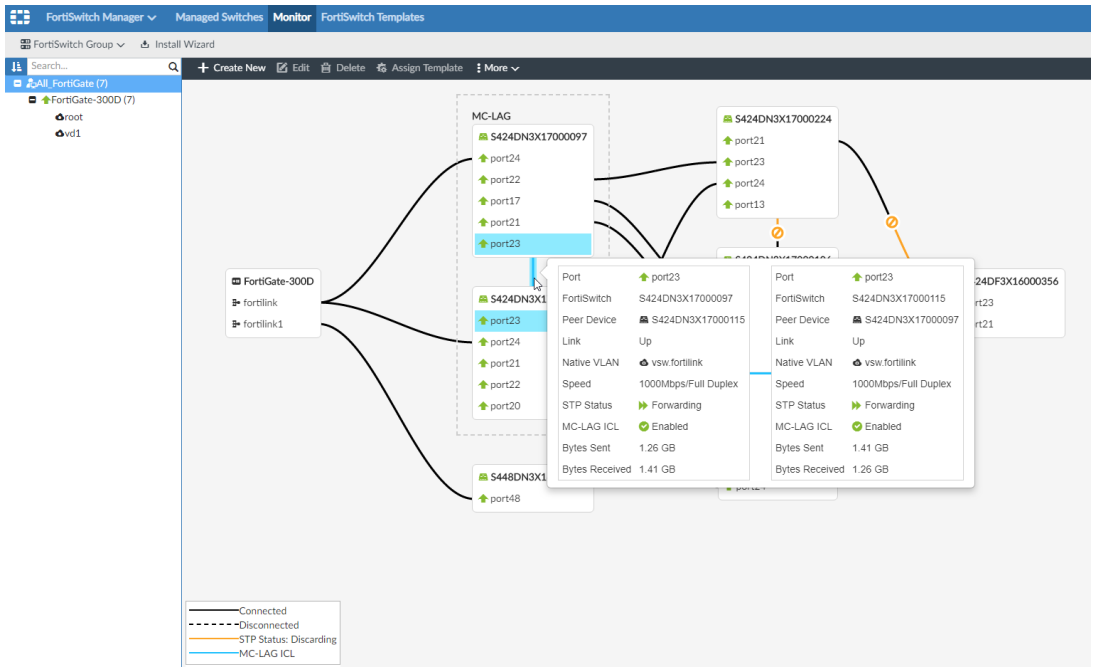
1. Hover over the connection between fortilink interface and the FortiSwitch to see the connection member information.



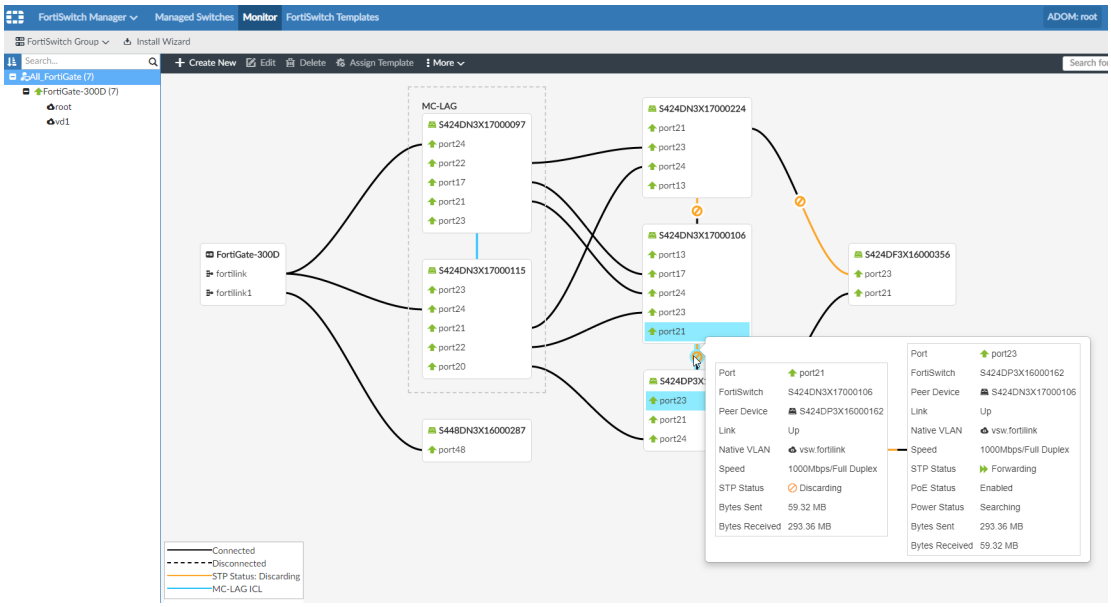
2. Hover over the connection between FortiSwitches, the connection member information is displayed.



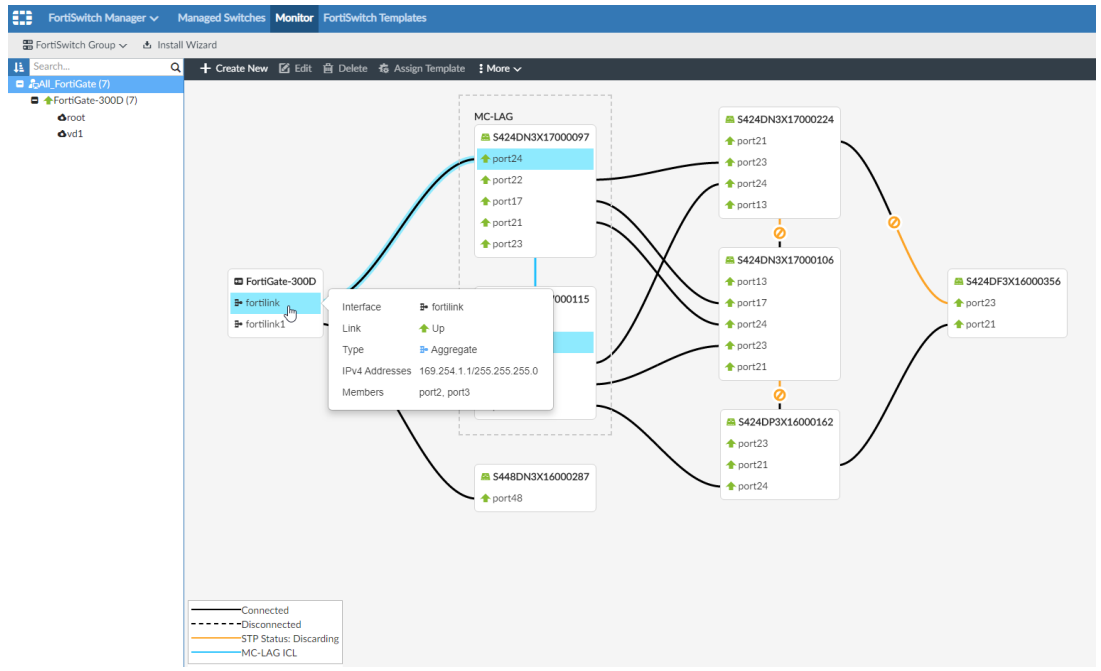
3. Hover over the MC-LAG ICL connection to see the related information.

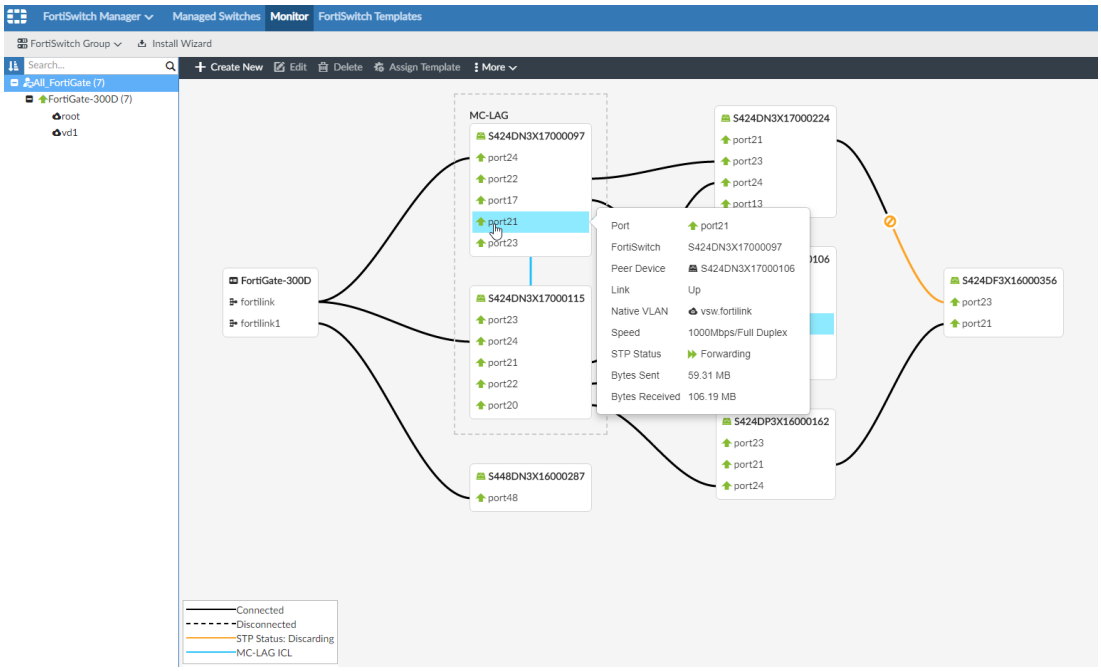


4. Hover over the STP discarding connection.
The connection information is available.

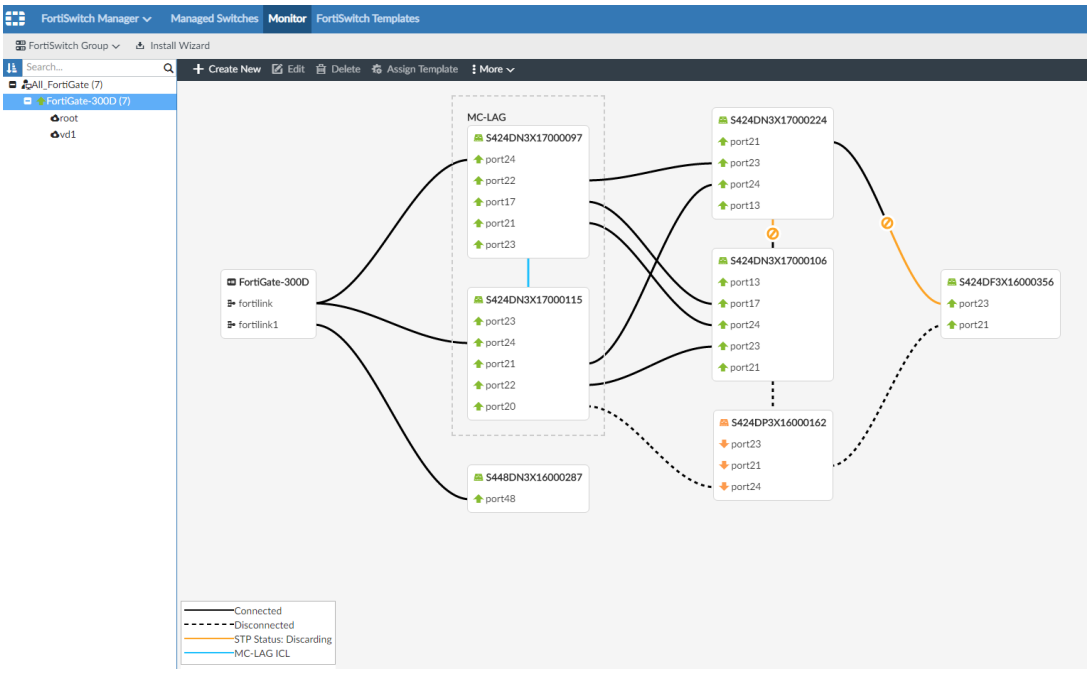


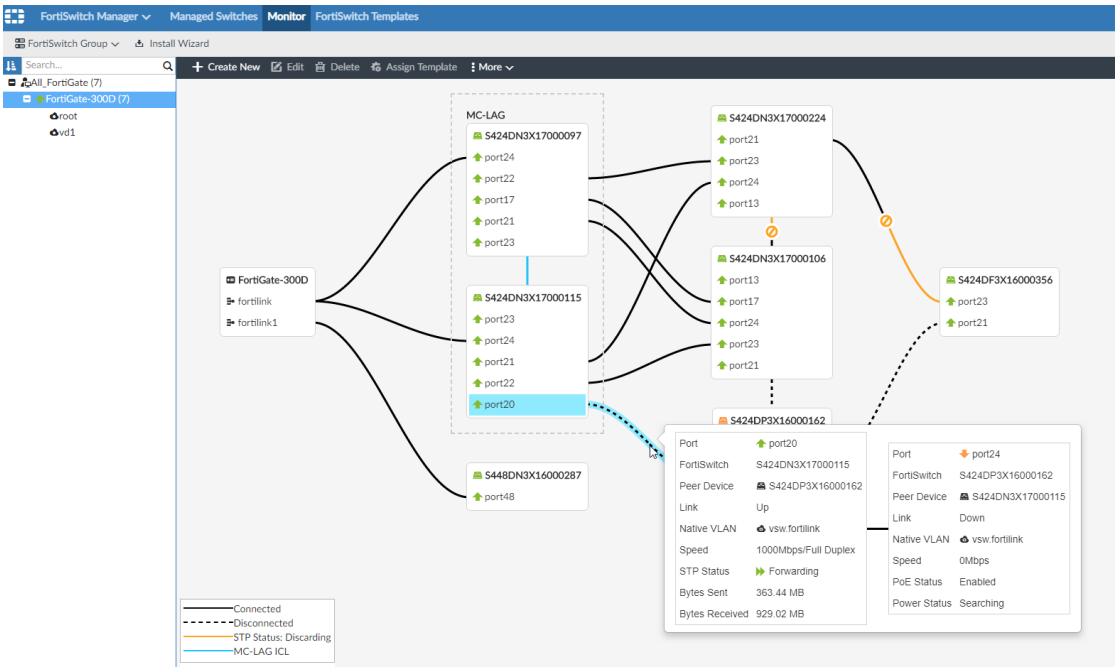
5. Hover over the FortiSwitch port or fortilink interface to see the port information.



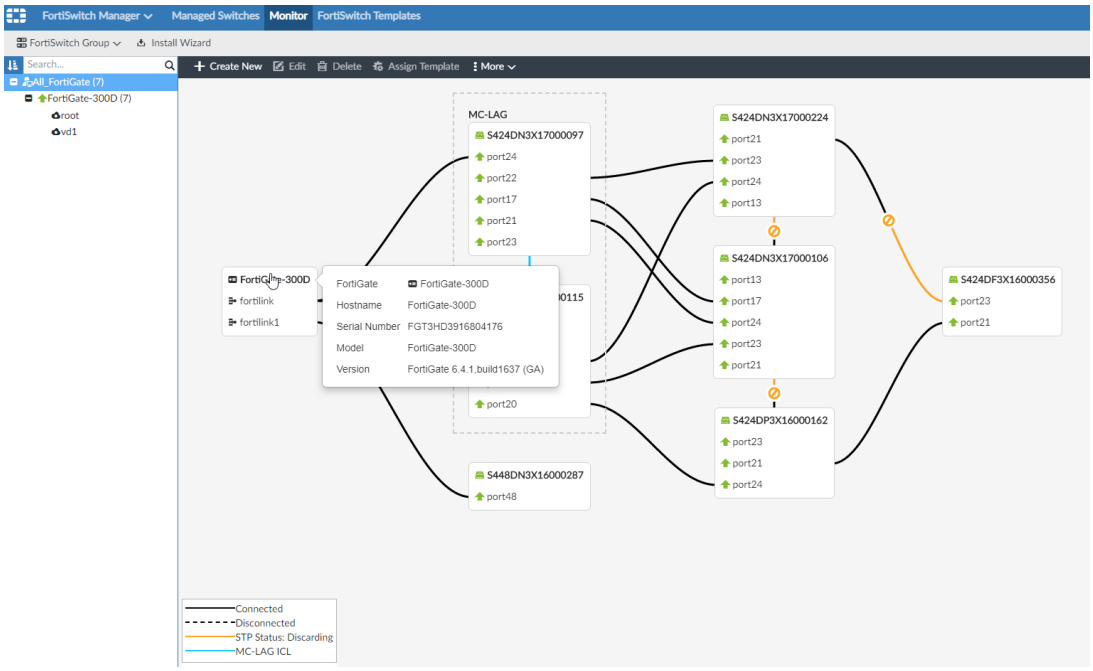


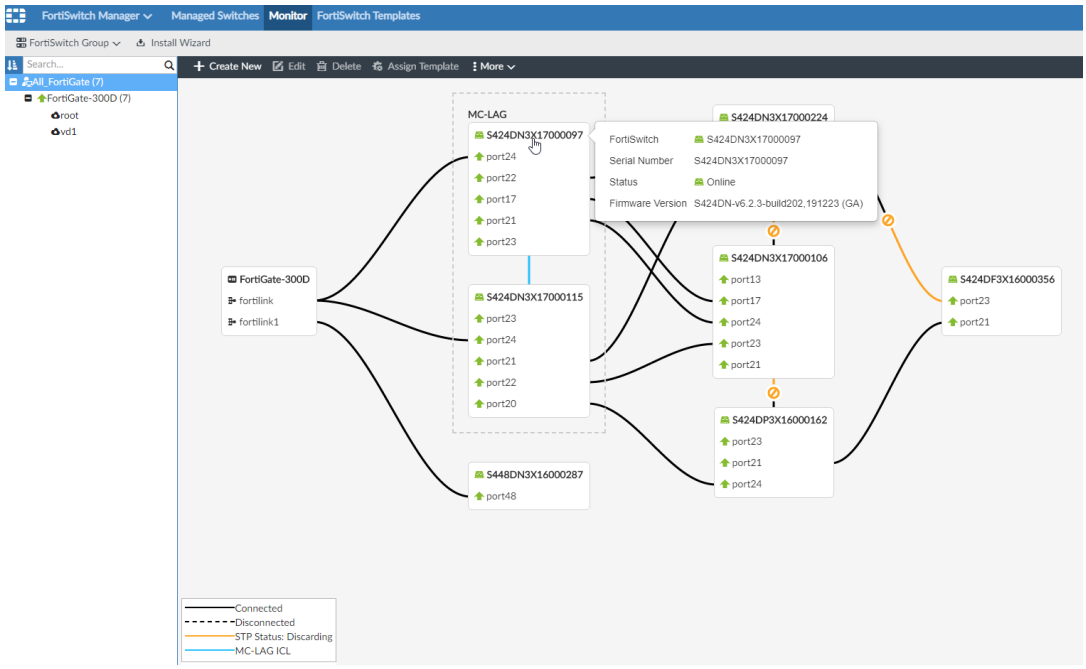
6. If the connection is unavailable, the link is disconnected.



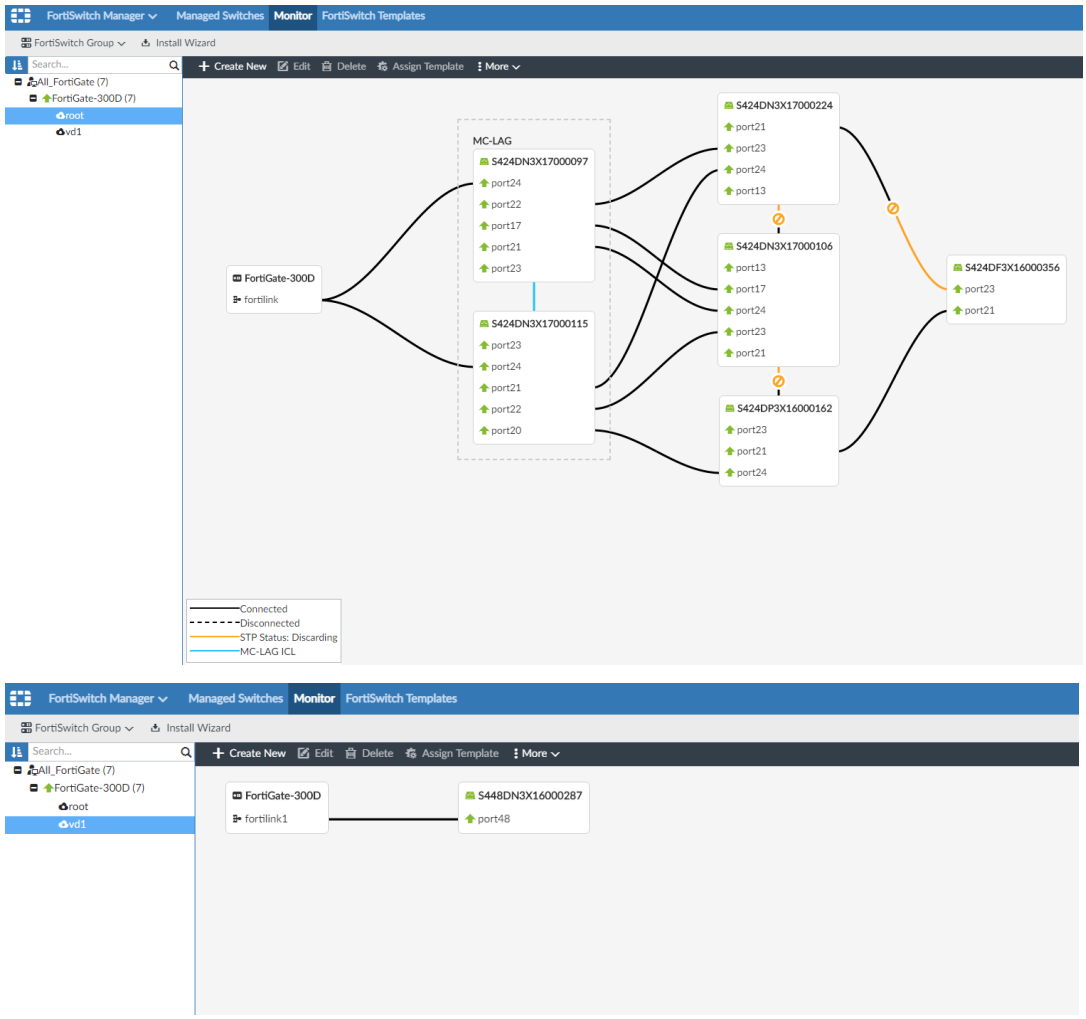


7. Hover over the FortiGate or FortiSwitch to see the related device information.





8. Choose a different VDOM in FortiGate, only the FortiSwitches in the selected VDOMs are displayed.



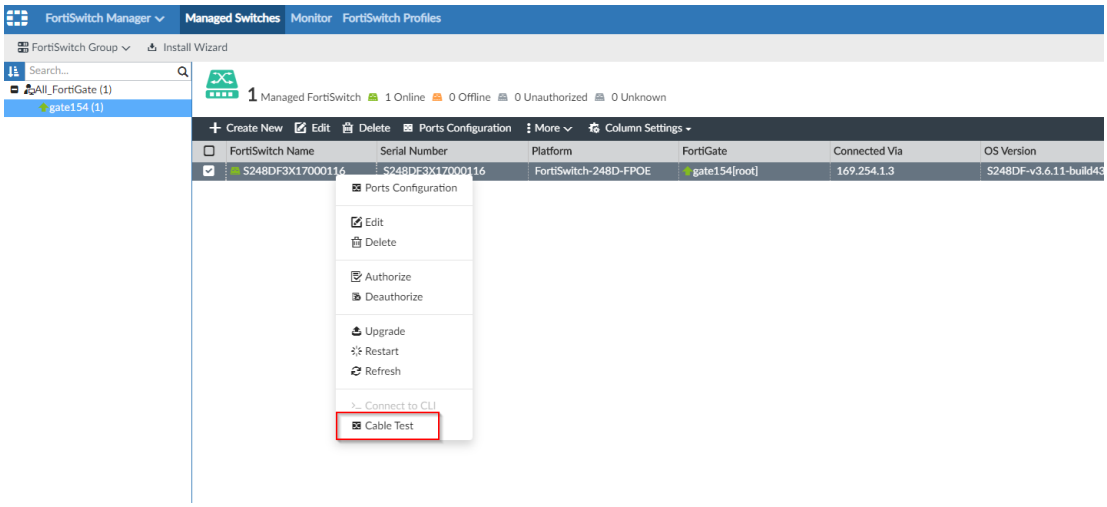
Run cable test on FortiSwitch ports from FortiManager- 6.4.2

You can trigger a FortiSwitch cable test from FortiManager.

The FortiSwitch cable test is only available on ADOM 6.4 and later.

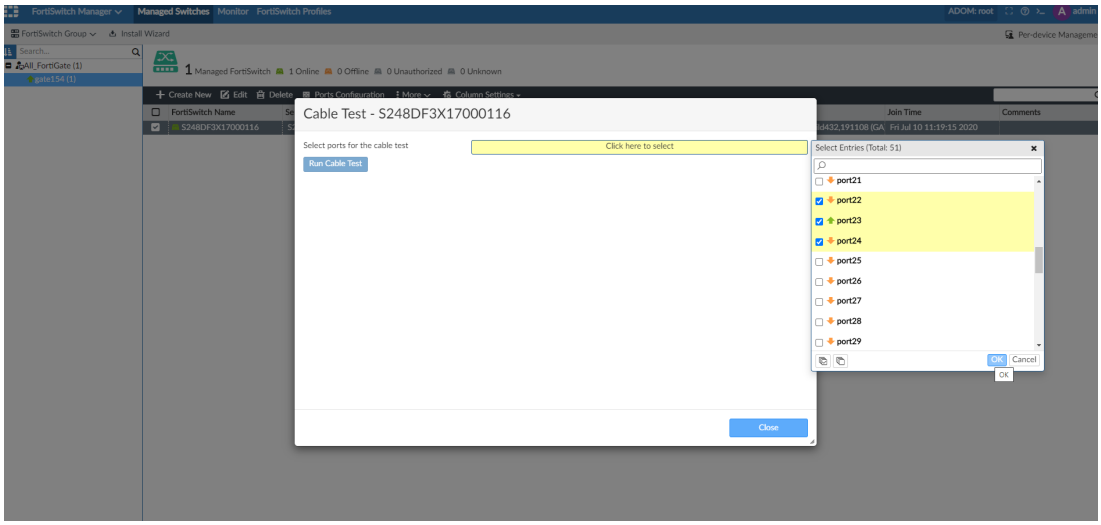
To perform a FortiSwitch cable test:

1. Go to *FortiSwitch Manager* > *Managed Switches*.
2. In the tree menu, select a FortiGate that contains the FortiSwitch on which the cable test is to be performed.
3. Select the FortiSwitch and either click *More* > *Cable Test* from the toolbar, or right-click the FortiSwitch and select *Cable Test*.



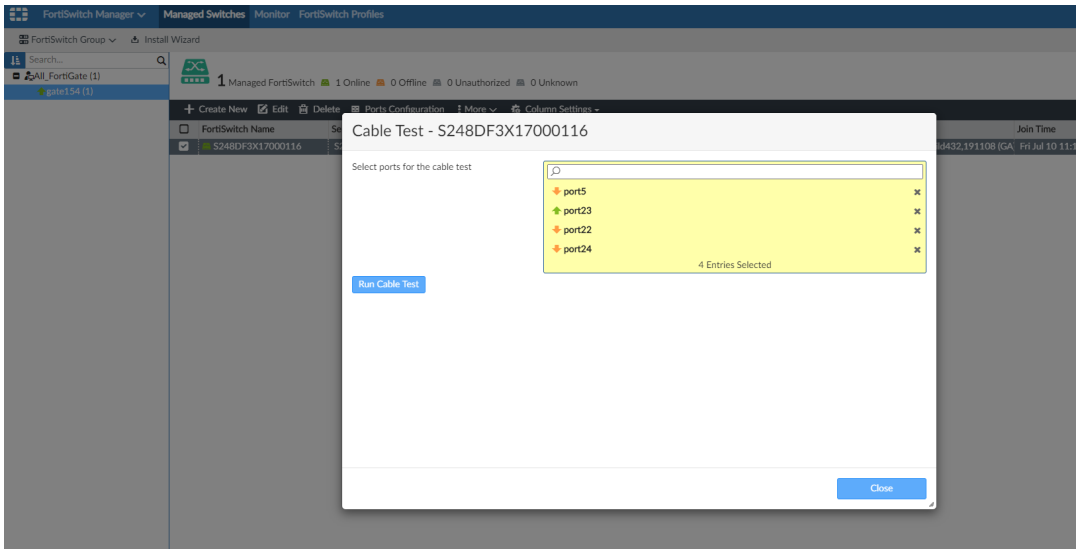
The *Cable Test* pane opens.

4. In the *Cable Test* pane, select the ports of the FortiSwitch you want to perform a cable test on, and click *OK*.

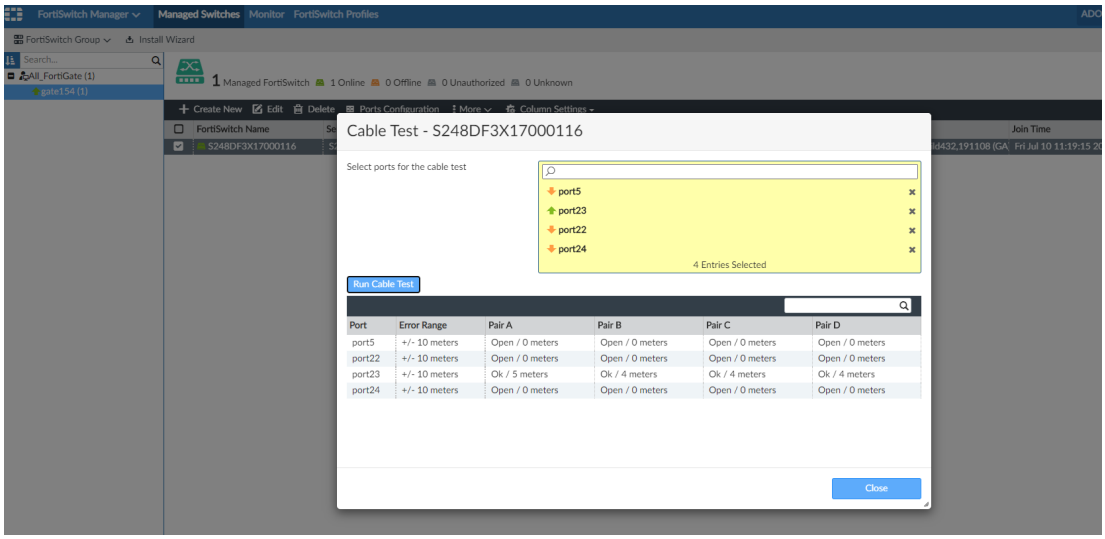


The *Select Entries* list does not contain FortiLink ports because cable test is not allowed for the FortiLink interface.

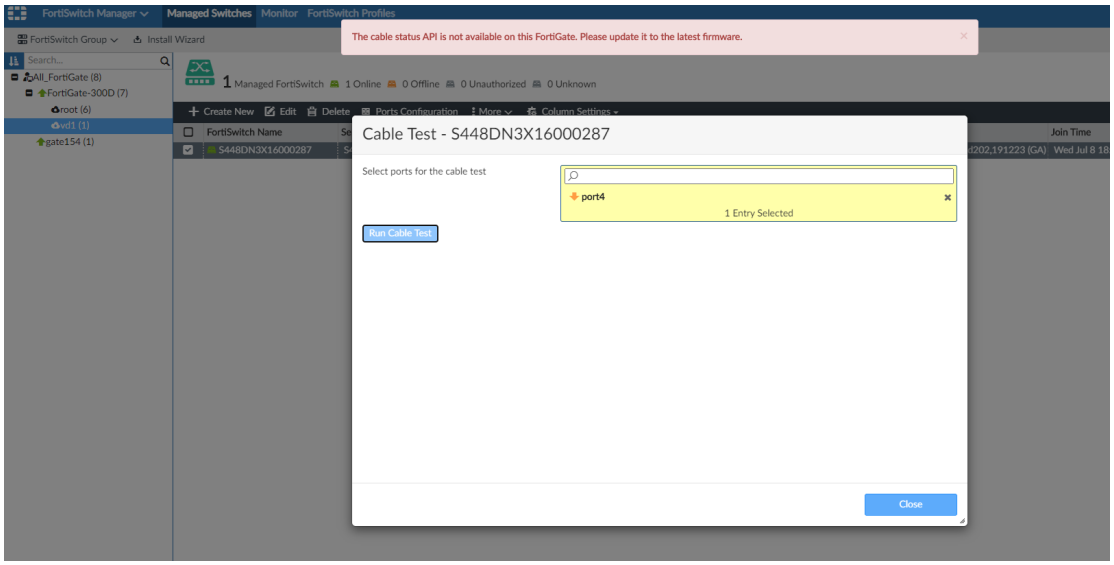
5. Click *Run Cable Test* to run the FortiSwitch cable test on the selected ports.



Once the cable test is finished, the results are displayed.



If the cable test API is not available for your version of FortiOS (6.4 branch, but build 1704 or earlier), an error prompt is displayed asking you to update to the latest firmware.

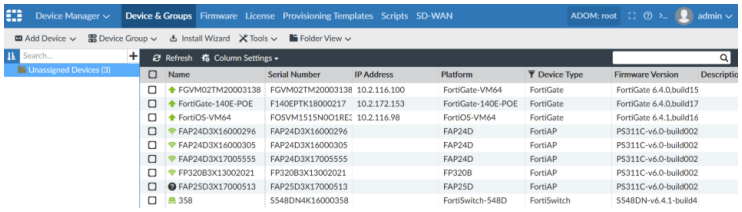


New Folder View added to display managed devices - 6.4.2

You can now organize devices within the tree menu in *Device Manager* to display FortiGates. The *Folder View* feature allows you to create, nest, and move folders in the tree menu. You can also move devices between folders.

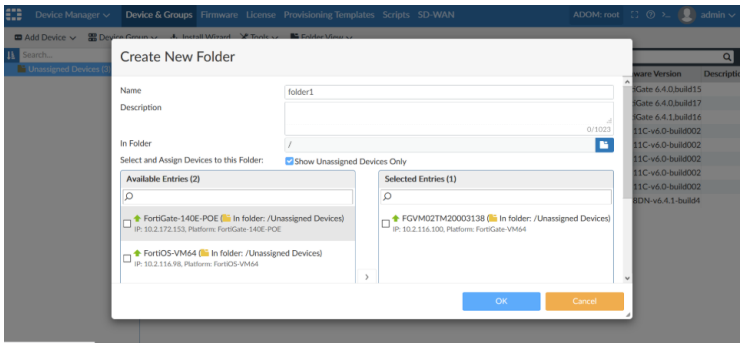
To access the new folder view:

1. Go to *Device Manager* > *Device & Groups*.
2. In the *Table View* dropdown menu, select *Folder View*.
   By default, all the devices are placed under *Unassigned Devices* in the tree menu.

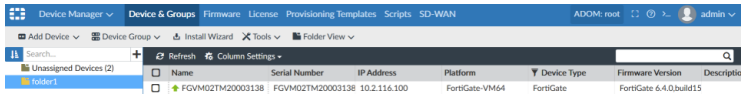


To create a folder:

1. Go to *Device Manager* > *Device & Groups*.
2. In the *Table View* dropdown menu, select *Folder View*.
3. To create a new folder, either click + beside the *Search* bar in *Folder View*, or right-click *Unassigned Devices*, and select *Create New Folder*.
   The *Create New Folder* dialog opens.



4. In the *Create New Folder* dialog, enter the name of the folder as folder1.
   Click *OK*.
   The new folder is created and visible in the tree menu. Also, the FortiGates in the folder are now displayed in the content pane.



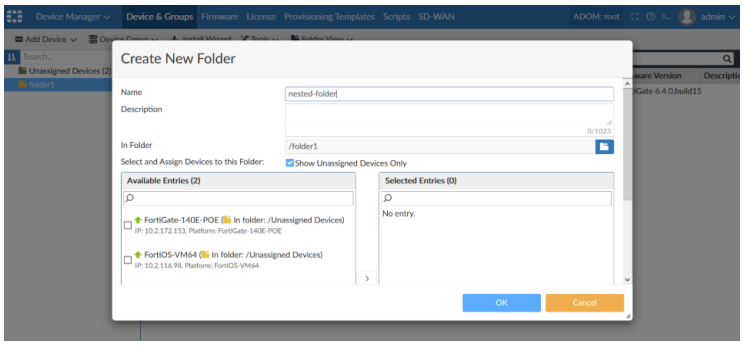
You can add FortiGates directly to a folder by selecting devices from the *Available Entries* list in the *Create New Folder* dialog.

Nested folders

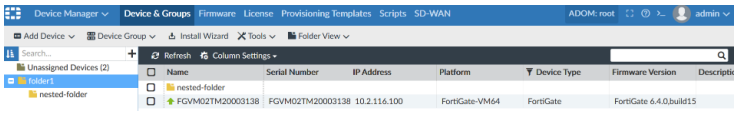
The new *Folder View* supports nested folders.

To create a nested folder:

1. In the tree menu, right-click the folder you intend to nest and select *Create New Folder*.
   For instance, right-click the previously created folder1 and select *Create New Folder*.
   The *Create New Folder* dialog opens.
   In Folder shows that the new folder will be created within folder1.

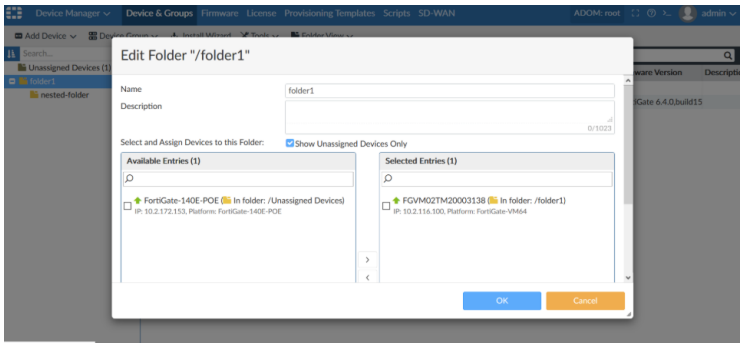


2. In the *Create New Folder* dialog, enter the name of the folder as nested-folder.
   Click *OK*.
   The nested-folder is created and displayed in the tree menu under the previously created folder1. Also, the folder and the FortiGates in the parent folder are displayed in the content pane.



To move FortiGates between folders:

1. Go to *Device Manager* > *Device & Groups*.
2. In the *Table View* dropdown menu, select *Folder View*.
3. In the tree menu, right-click the folder where the FortiGate is to be moved, and select *Edit*.
   The *Edit Folder* dialog opens.



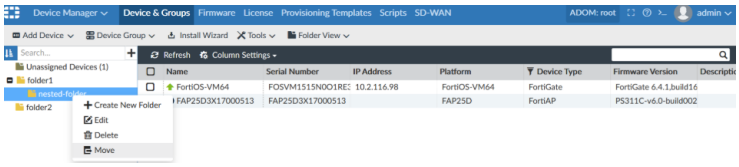
4. In the *Edit Folder* dialog, select the FortiGate to be moved from the *Available Entries* list.
   Click *OK* .

Alternatively, from the *Device & Groups* pane, select a FortiGate, drag and drop it to the folder where you want to move the selected FortiGate.

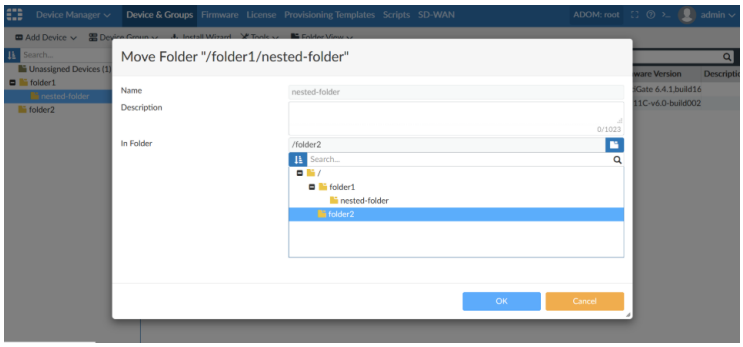
At any given time, a FortiGate can only be added to one folder.

To move a folder:

1. Go to *Device Manager* > *Device & Groups*.
2. In the *Table View* dropdown menu, select *Folder View*.
3. In the tree menu, right-click the folder you want to move, here nested-folder, and select *Move*.
   The *Move Folder* dialog opens.

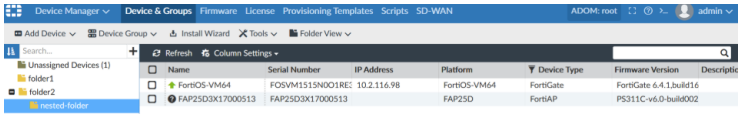


4. In the *Move Folder* dialog, under *In Folder*, select the destination folder, here folder2.



Click *OK*.

The nested-folder moves to folder2 including folders and devices in it.

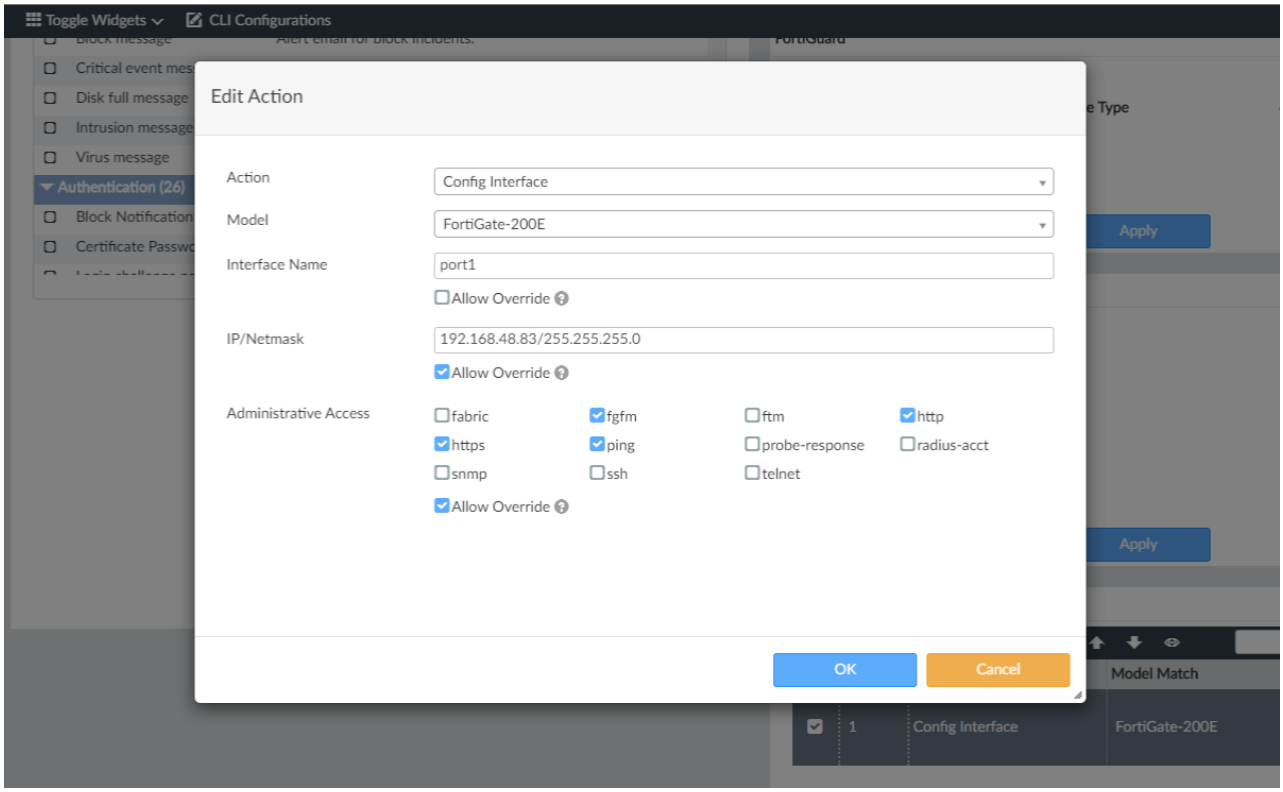


Model device approval using device template - 6.4.2

With FortiManager 6.4.2, you can now add a model device using a device template. You can either use a site template or a provisioning template to add a model device.

To add a model device using a provisioning template:

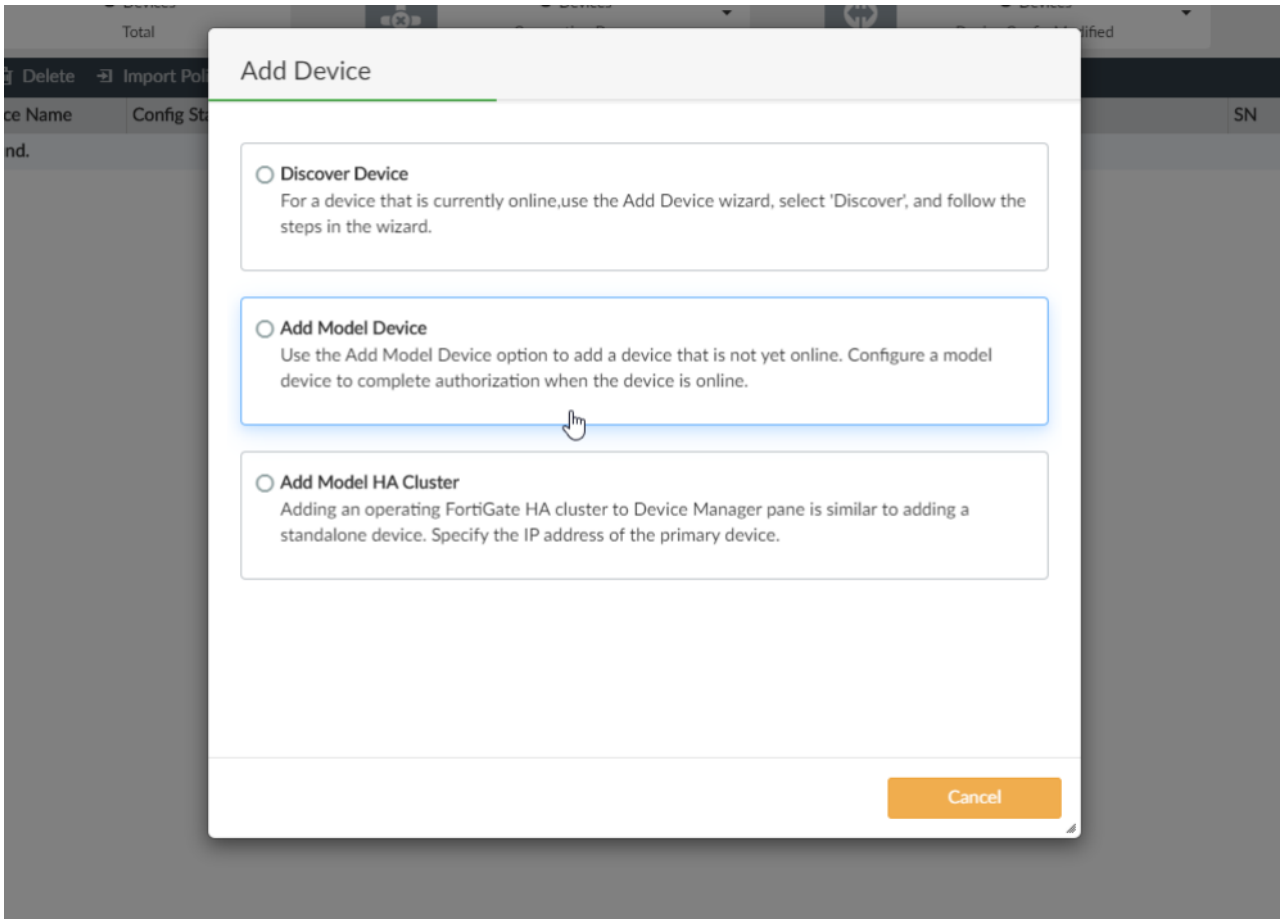
1. Go to *Device Manager* > *Provisioning Templates* > *System Templates*, and create a new provisioning template.



The *Allow Override* option allows overriding profile values when using a provisioning template to add a model device. Use the option while creating a template to override any profile values later when you add a model device using a provisioning template. If the option is left unchecked, you cannot override profile values when adding a model device using a provisioning template.

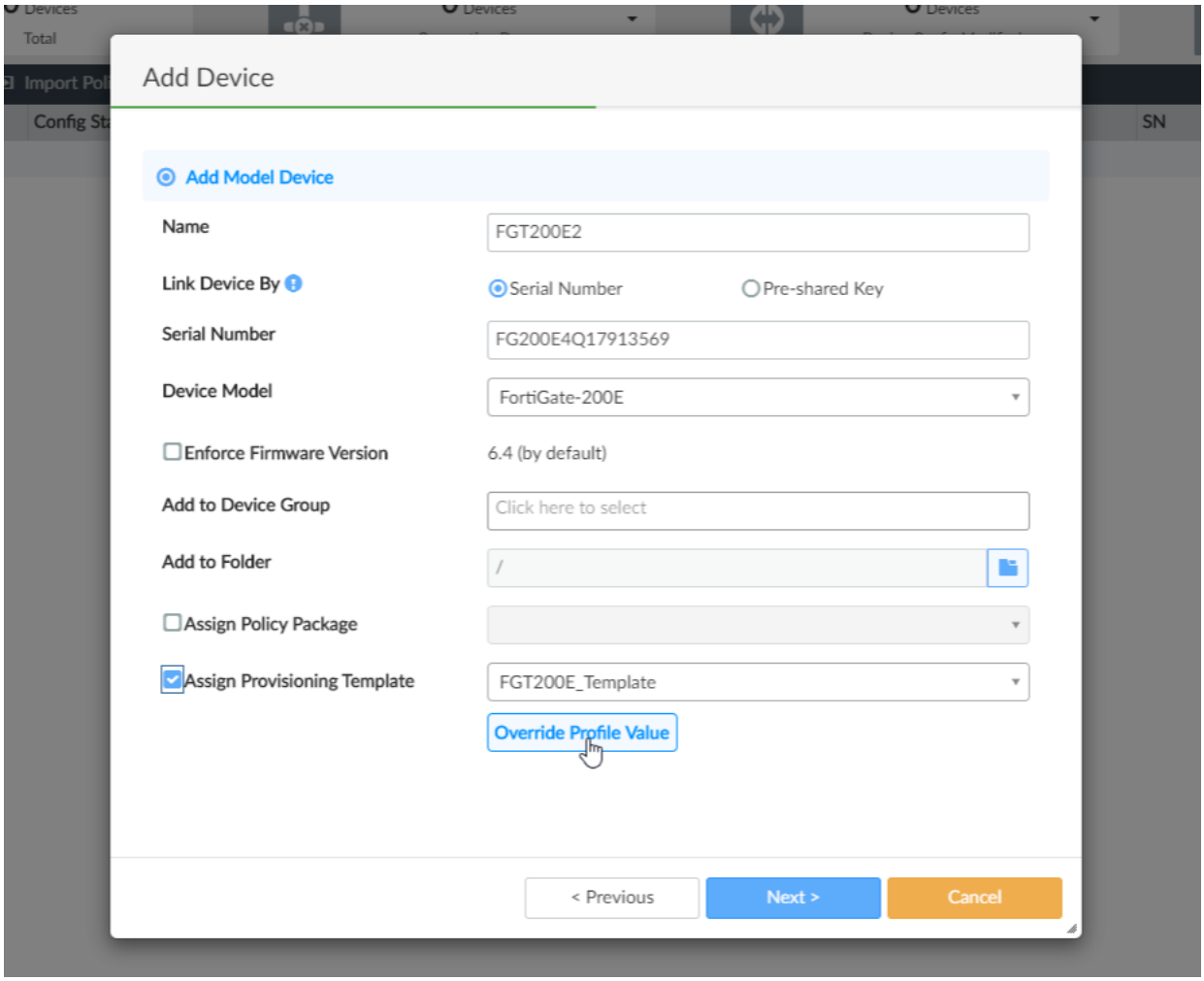
2. Go to *Device Manager* > *Device & Groups* > *Add Device*. The *Add Device* dialog appears.

3. Click *Add Model Device*.



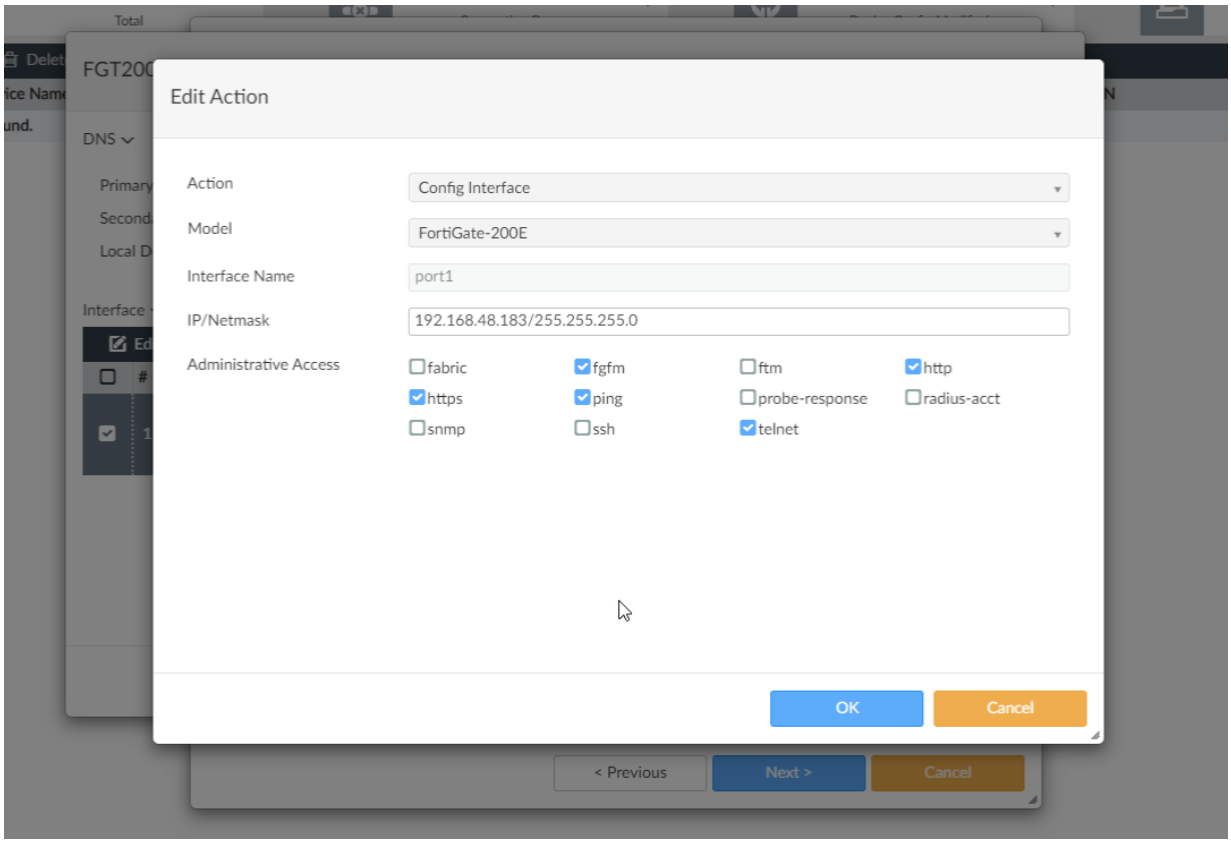
4. Configure the settings as follows:

Name	Enter a name for the model device.
Link Device By	Select *Serial Number*.
Serial Number	Add the serial number of the FortiGate device to be added.
Device Model	Select the device model from the drop-down list.
Assign Provisioning Template	Select the provisioning template you created in Step 1 from the drop-down list.



To continue without overriding the profile values, proceed with the next steps. To override profile values in the provisioning template:

a. Click *Override Profile Value*. The template widget override dialog appears.
b. Select the interface and click *Edit*. The *Edit Action* dialog appears.

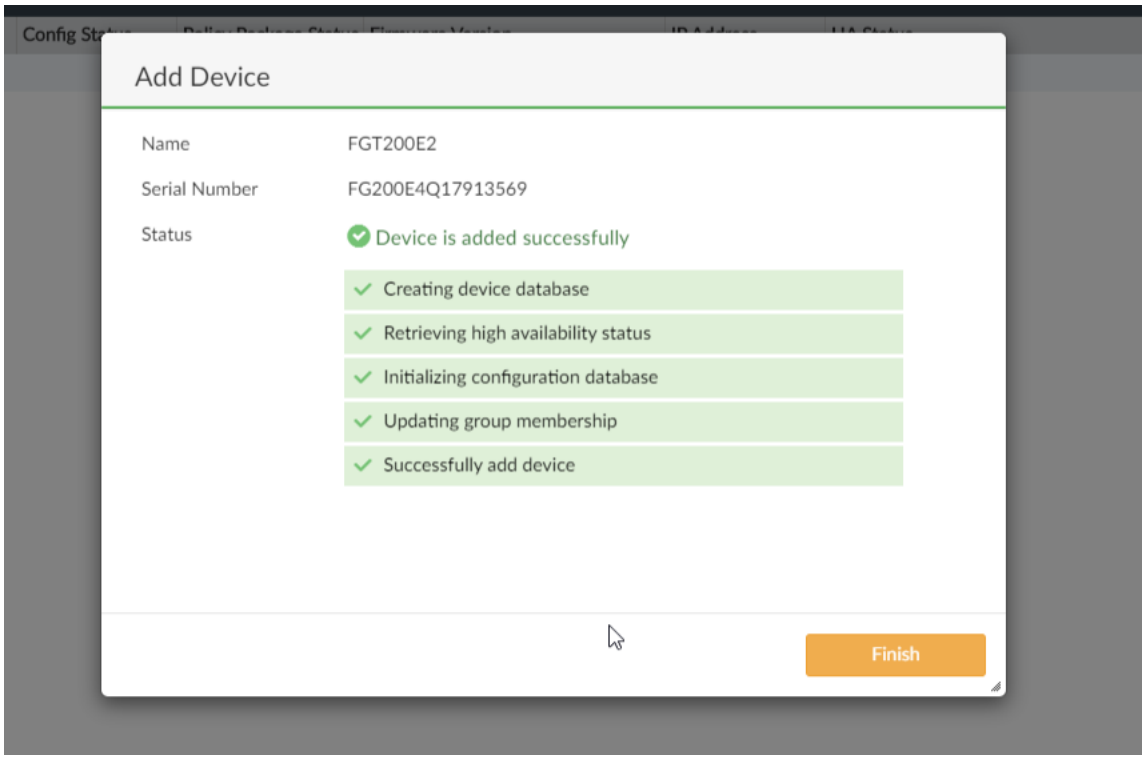


c. Make the required changes and click *OK*.

You can only change the fields that were configured with the *Allow Override* option while creating the template. If the option was left unchecked, you cannot override profile values when adding a model device using a provisioning template.

d. The profile values have successfully been overridden. Click *OK*.

5. Click *Next*. The device is successfully added.



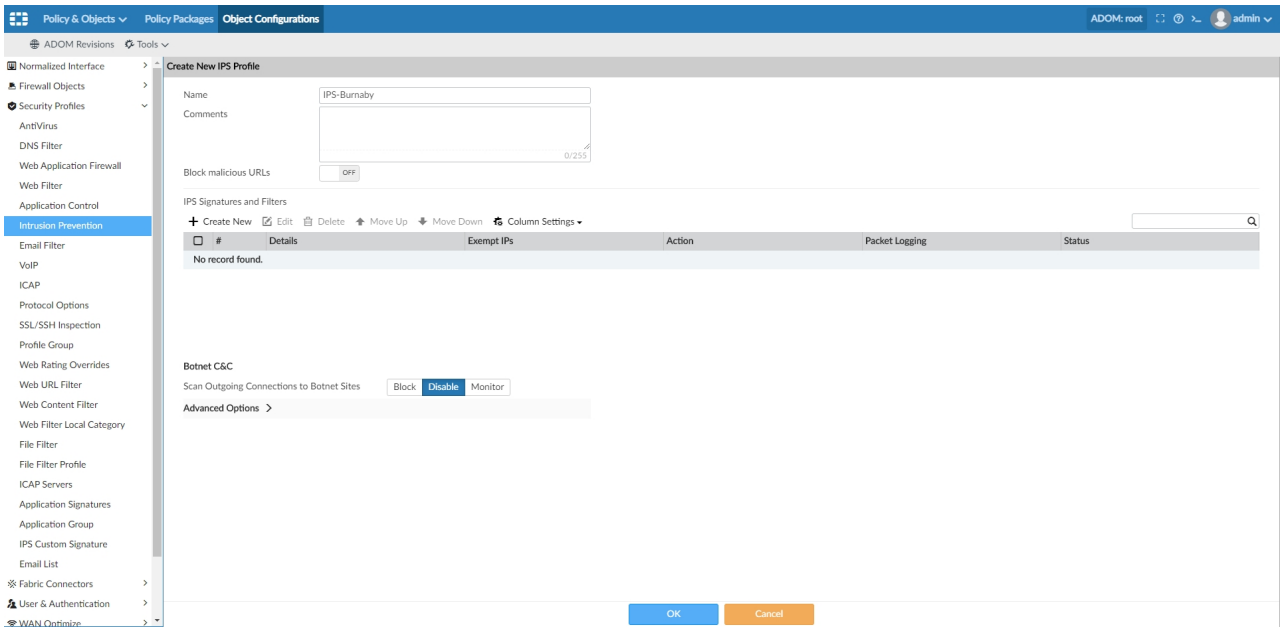
6. On the added FortiGate device, add the FortiManager IP address.
7. Confirm the FortiGate on the FortiManager to synchronize both the devices. The provisioning template, along with profile overrides if any, is pushed to the FortiGate device.

IPS signature activation filter: hold-time and CVE pattern - 6.4.2

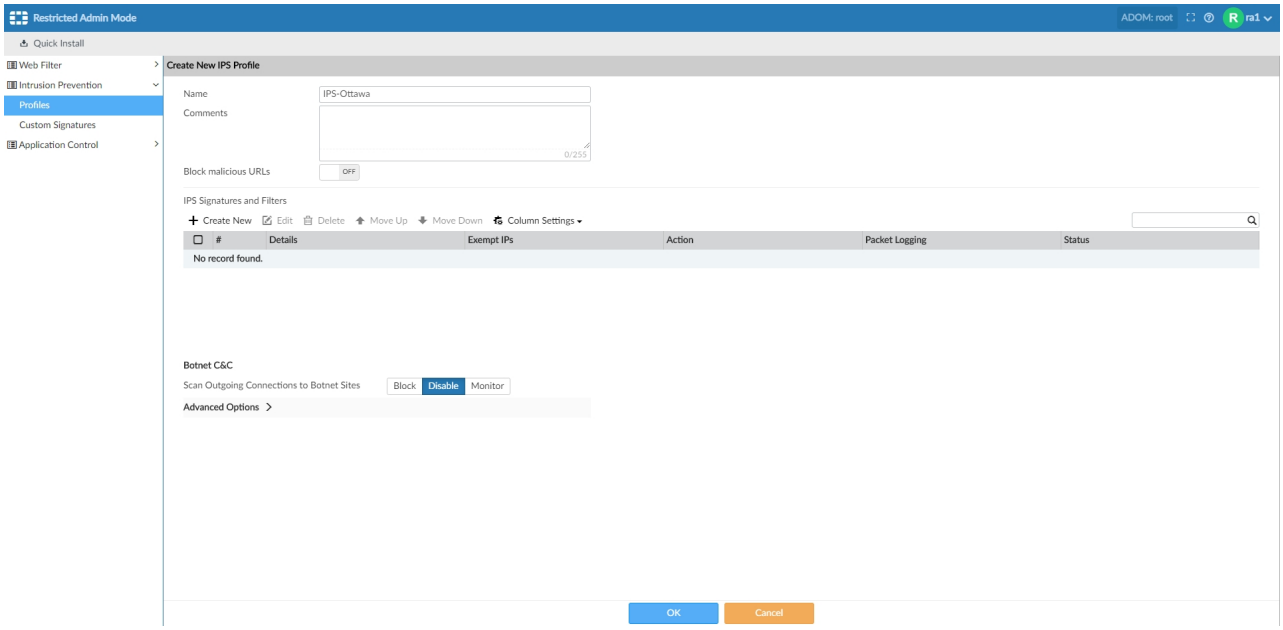
FortiManager now supports CVE ID filtering. You can also set the hold-time for an IPS signature activation.

To add a CVE filter in the GUI:

1. Log into FortiManager as a System Admin or Restricted Admin.
   If you are logged in as System Admin, go to *Policy & Objects* > *Object Configurations* > *Security Profiles* > *Intrusion Prevention*.

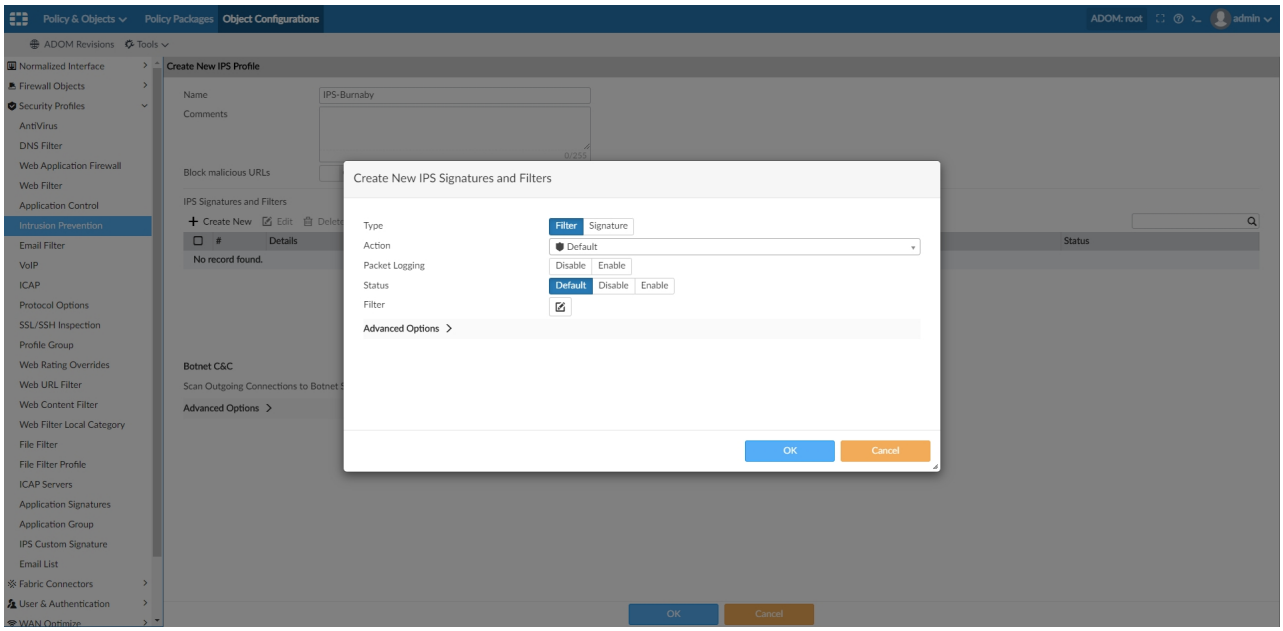


If you are logged in as a Restricted Admin, go to *Intrusion Prevention* > *Profiles*.

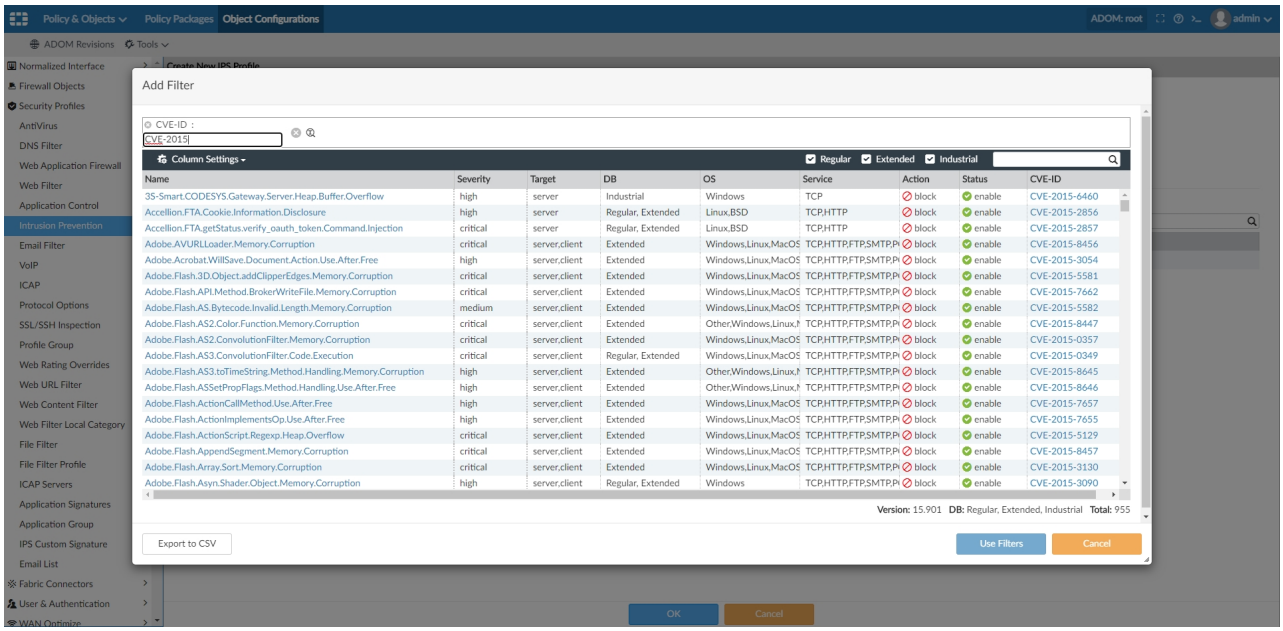


2. In the *IPS Signatures and Filters* section, create a new filter or select a filter to update. The *Create New IPS Signatures and Filters* dialog box is displayed.

3. Click the *Filter* icon.



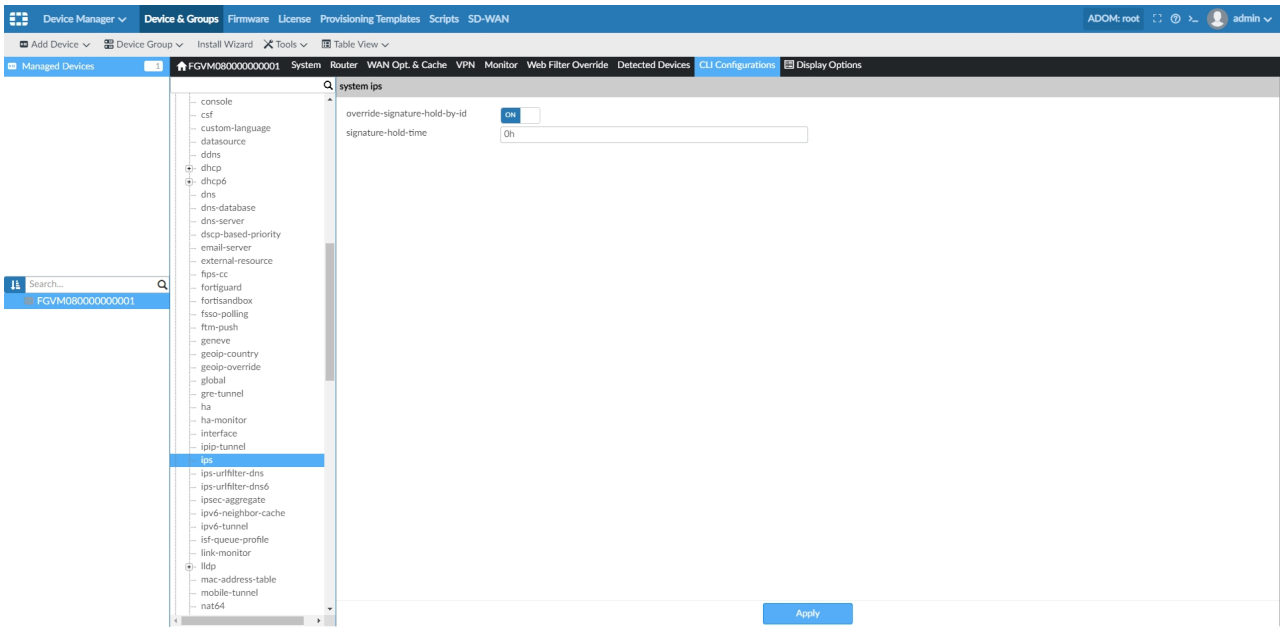
4. Click *Add Filter* > *CVE ID*. Enter the CVE ID, then click *Use Filters*, and click *OK*.



To configure the hold-time settings in the GUI:

1. Go to *Device Manager* > *Device & Groups*.
2. Select a managed device.
3. In the toolbar, click *CLI Configuration*.
4. In the configurations menu, go to *System* > *IPS*. The *system ips* dialog box is displayed.

5. Ensure *override-signature-hold-by-id* is enabled.



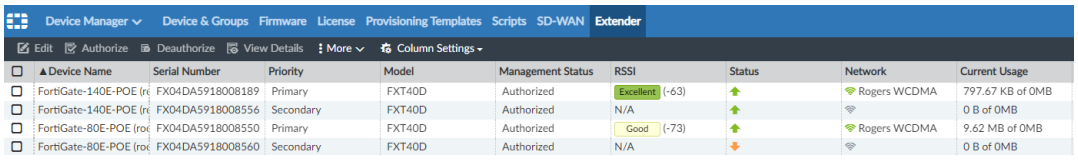
6. In the *signature-hold-time* field, enter the number of days or hours hold and monitor the IPS signatures.

Display RSSI signal information and connection status for a managed FortiExtender - 6.4.2

You can now see GSM signal information and the LTE connection status extracted from a FortiExtender and managed by a FortiGate in FortiManager.

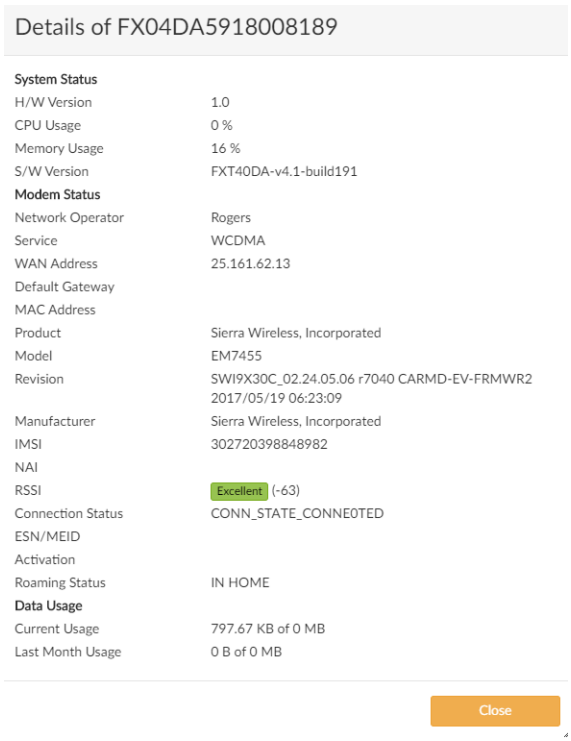
To display FortiExtender signal information:

1. Go to *Device Manager* > *Extender*.
   The managed FortiExtenders and their RSSI signal information is displayed.



If there is no SIM inserted, *N/A* is displayed.

2. Select a FortiExtender and click *View Details* in the toolbar, or right-click the FortiExtender device, and select *View Details*.
   The *Details* pane opens.
   Status information including system status, modem status, and data usage are displayed.



Note: For reference, the signal strength bands are derived from the following chart:

		RSSI	SINR (dB)	RSRQ (dB)	RSRP (dB)	EC/Io (dB)
	Technology	LTE amd 3G	LTE only	LTE only	LTE only	HSPA+ and EVDO
Signal Quality	Excellent	> -65	> 12.5	> -5	> -84	> -2
	Good	-65 to -75	10 to 12.5	-6 to -10	-85 to -102	-2 to -5
	Fair	-75 to -85	7 to 10	-6 to -10	-103 to -111	> -2
	Poor	< -85	< 7	< -11	< -112	< -10

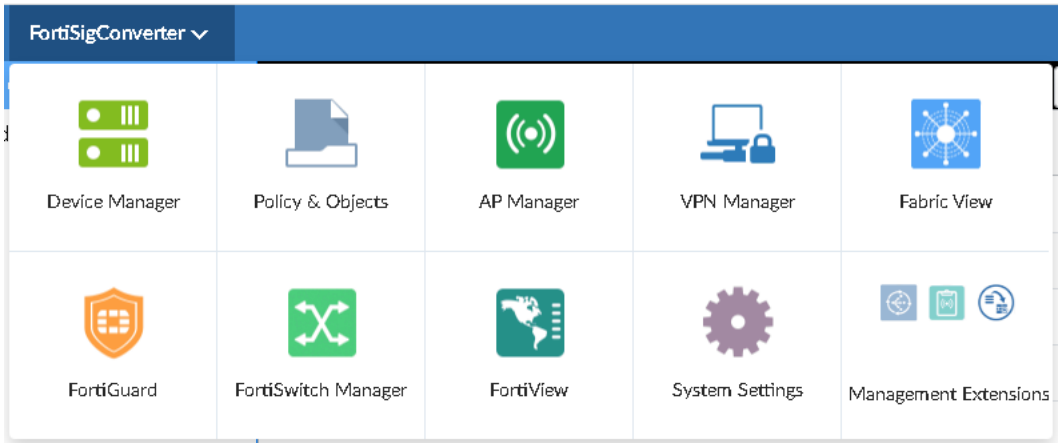
FortiSigConverter management extension tool to import Snort rules - 6.4.3

FortiManager supports Snort, a popular open source Network Intrusion Detection System (NIDS), using the FortiSigConverter application.

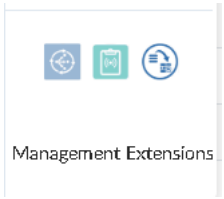
You can download FortiSigConverter from `registery.fortinet.com` directly in FortiManager using the *Management Extensions* module.

To enable FortiSigConverter in the GUI:

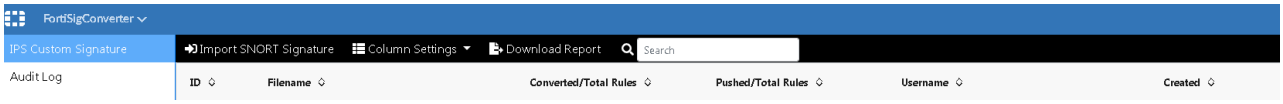
1. Go to *Management Extensions*.



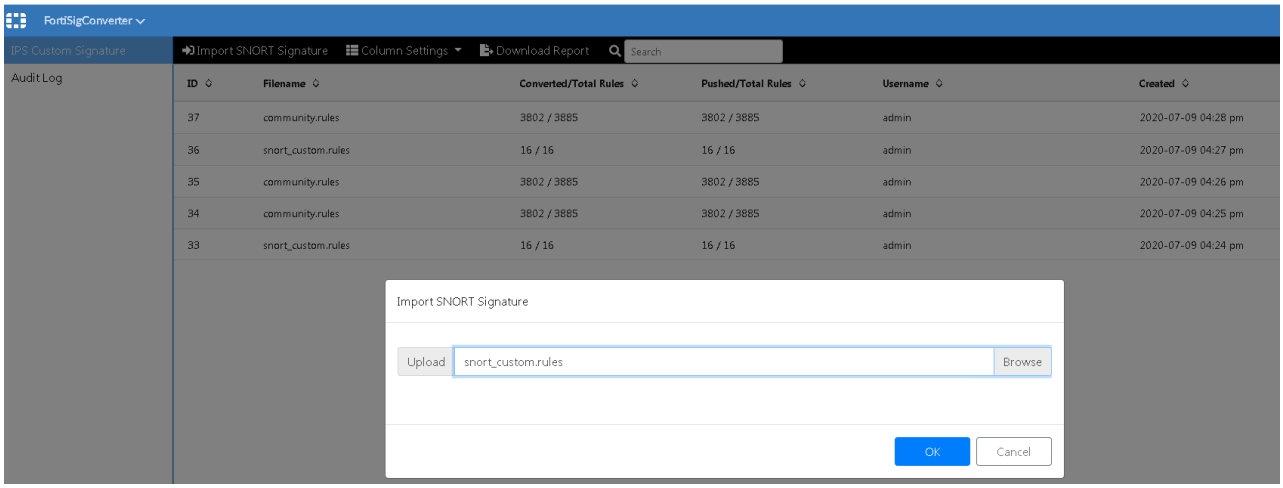
2. Click *FortiSigConverter* to download the management extension, and then open the application.



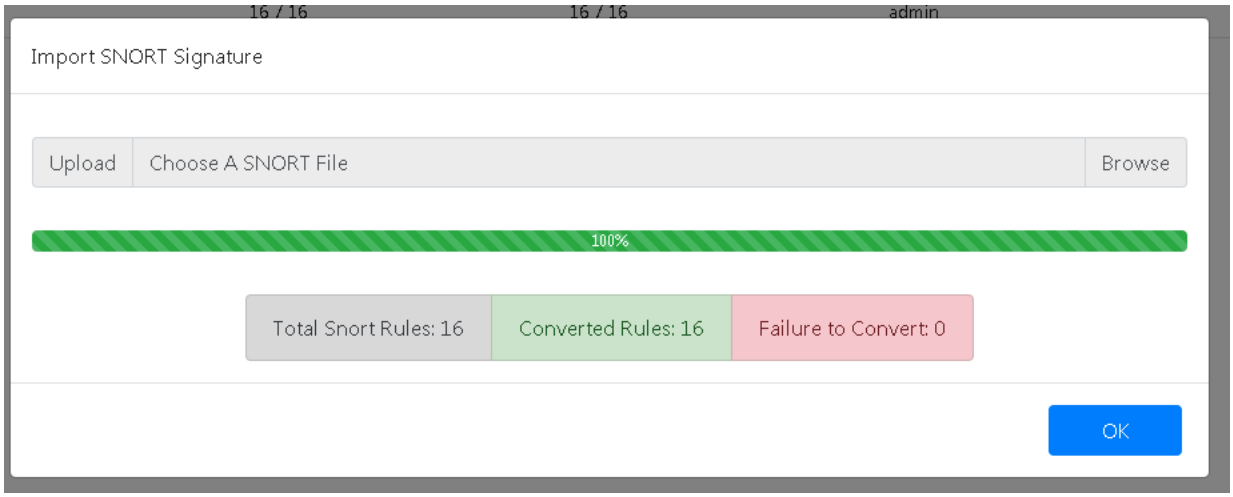
The FortiSigConverter dashboard is displayed.



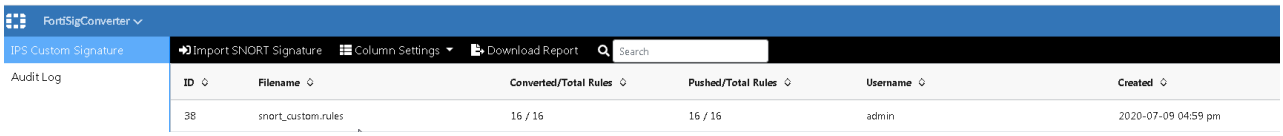
3. To import a signature file, click *Import SNORT Signature*, and click *OK*.



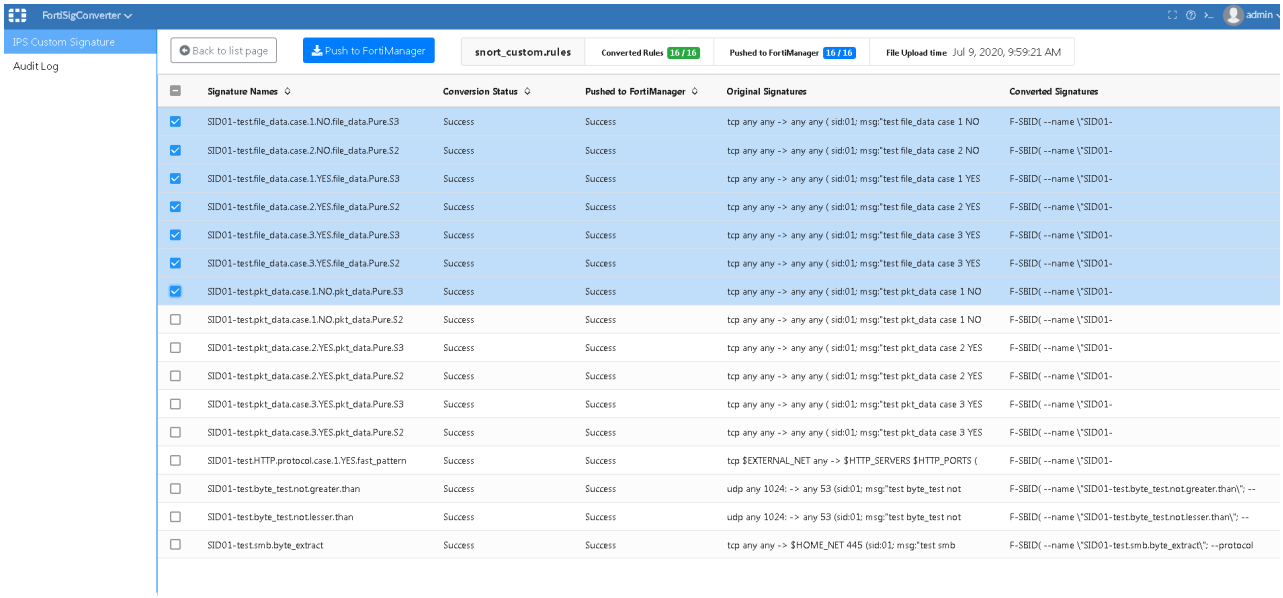
4. Click *OK* to confirm the import.



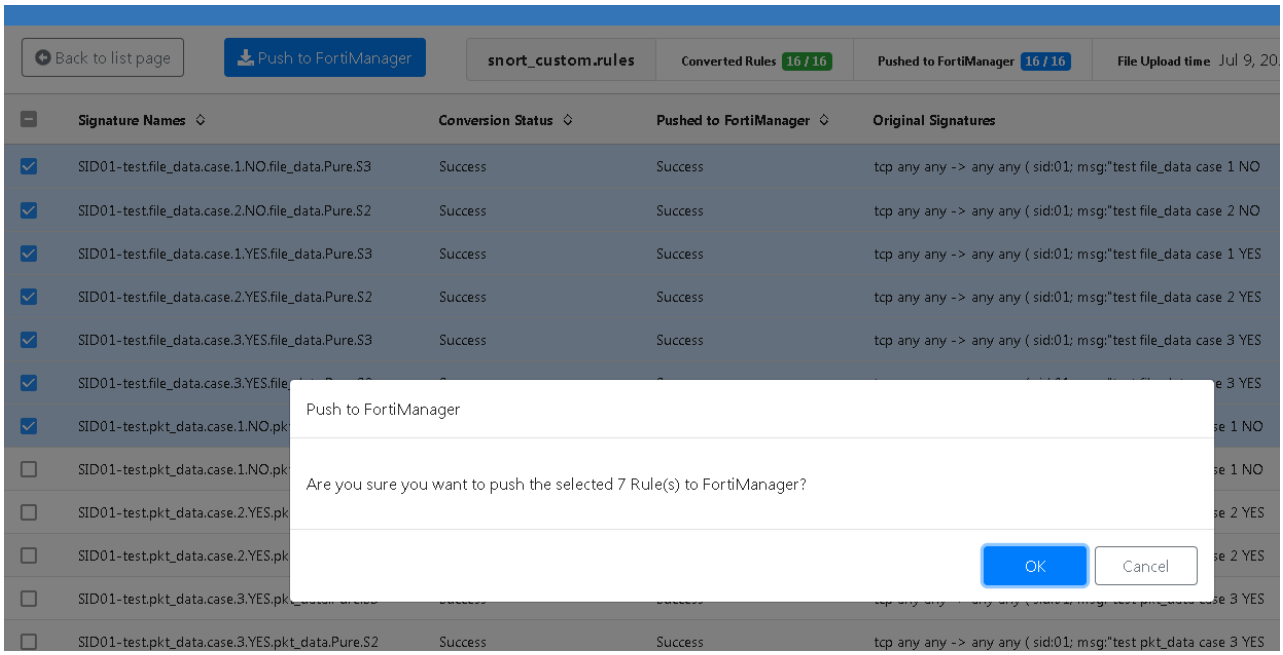
The signatures are added to the signatures list.



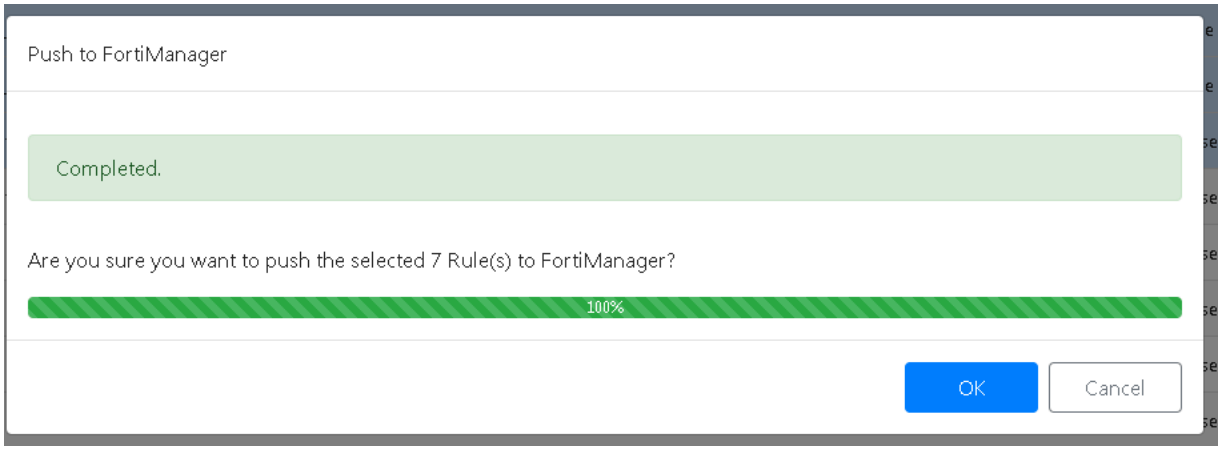
5. To push Snort rules to FortiManager, open a signature file and select the rules you want to push.



6. Click *Push to FortiManager*, and click *OK*.

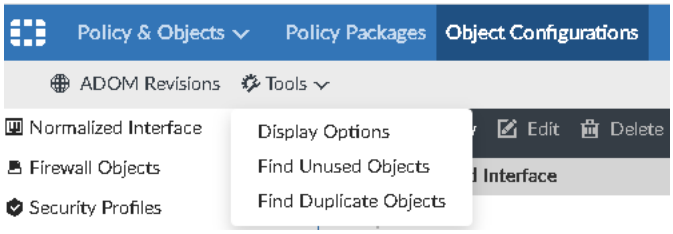


7. Click *OK* in the dialog box to complete the process.

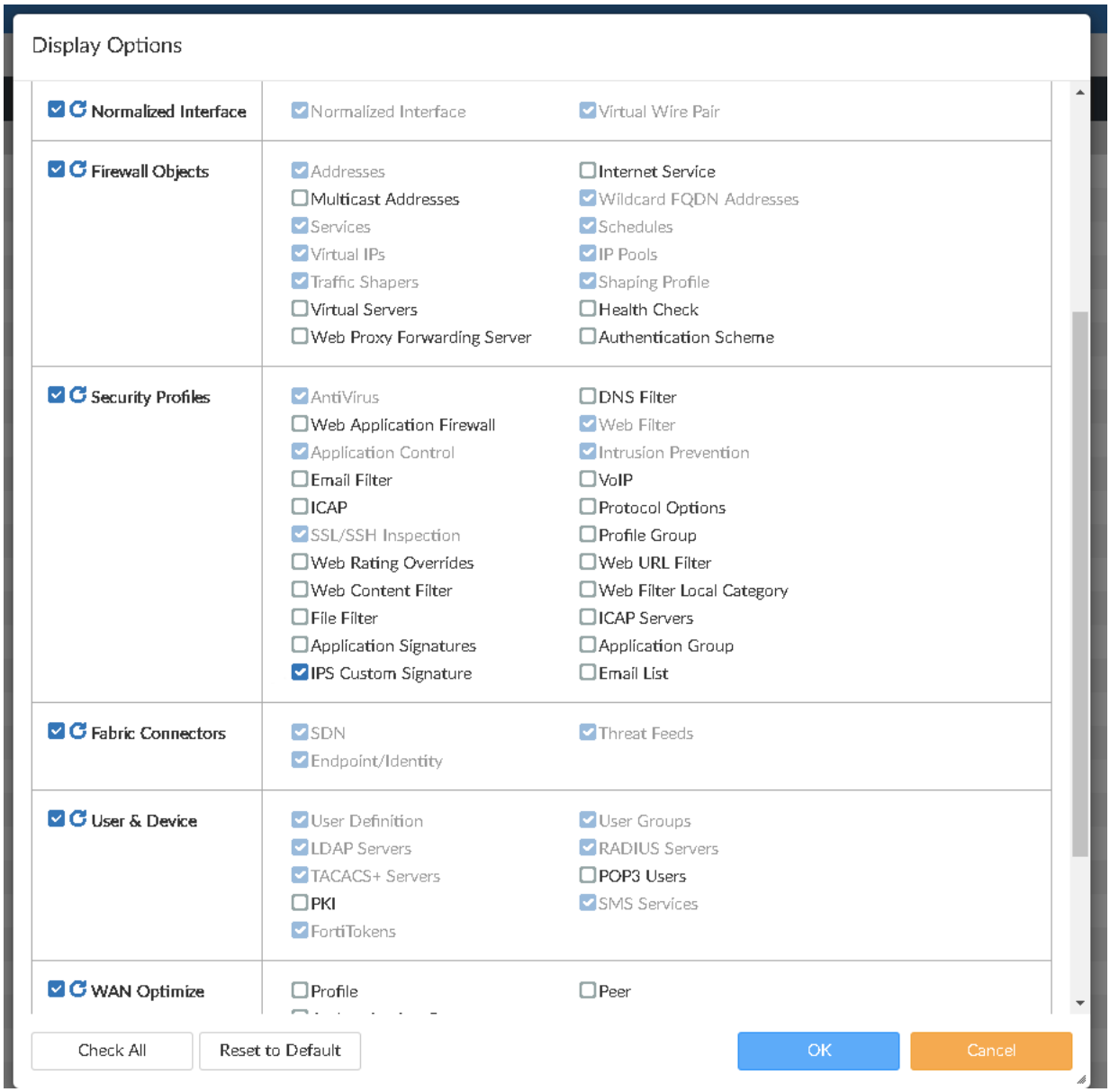


To view IPS signatures in FortiManager:

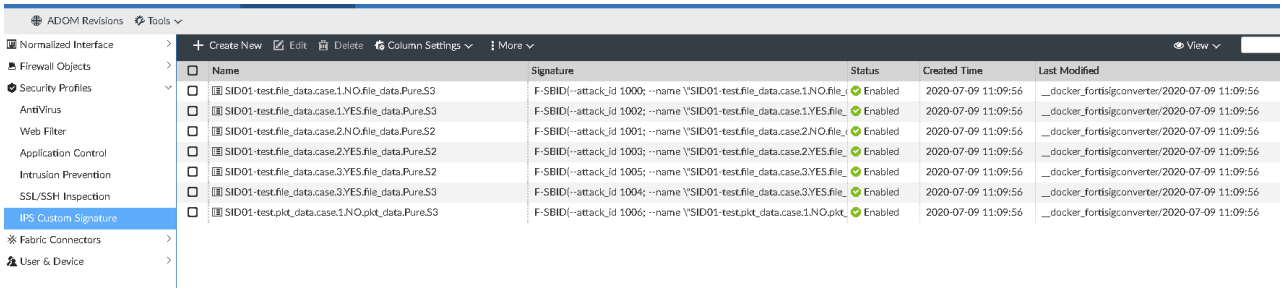
1. In FortiManager, go to *Policy & Objects* > *Object Configuration*.
2. Click *Tools* > *Display Options*.



3. In the *Security Profiles* module , select *Enable IPS Custom Signature*.



4. To view the signatures, go to *Security Profiles* > *IPS Signatures*.



To enable FortiSigConverter in the CLI:

```
config system docker
```

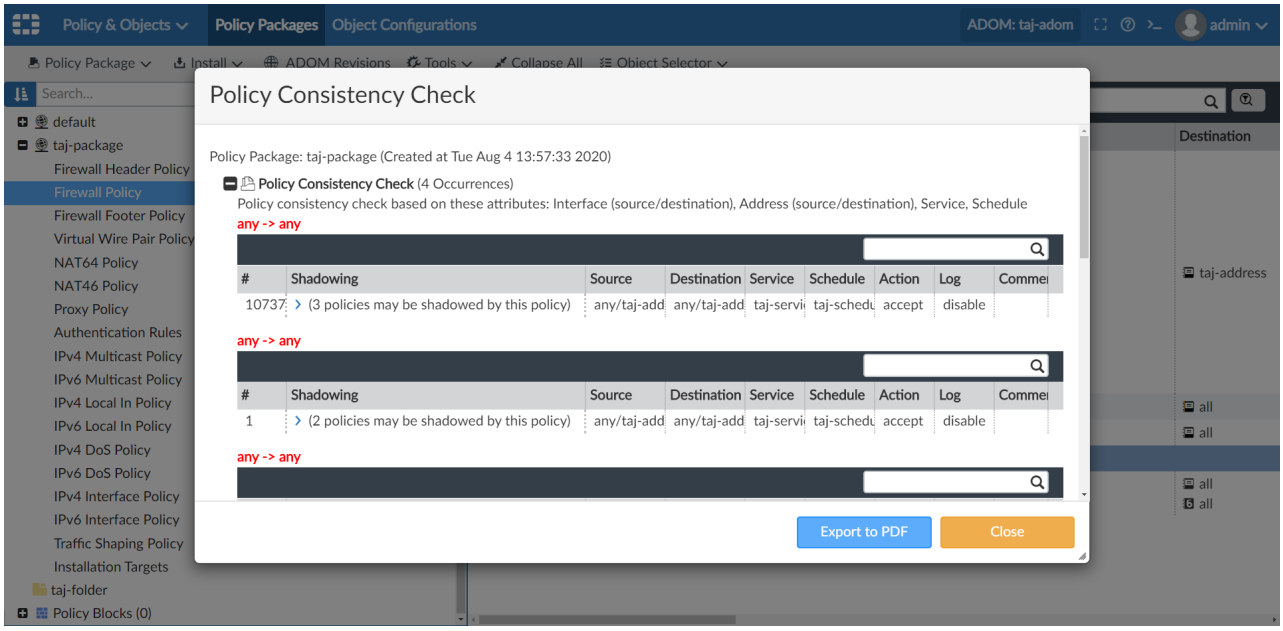
```
    set fortisigconverter enable
end
```

Export policy check results - 6.4.3

You can use the GUI to export Policy Check results as a PDF.

To export the results from a policy check in the GUI:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package or folder, and from the *Policy Package* menu, select *Policy Check*. The *Policy Consistency Check* dialog box opens.
4. To perform a new consistency check, select *Perform Policy Consistency Check*, then click *OK*.
   A policy consistency check is performed, and the results screen is shown.



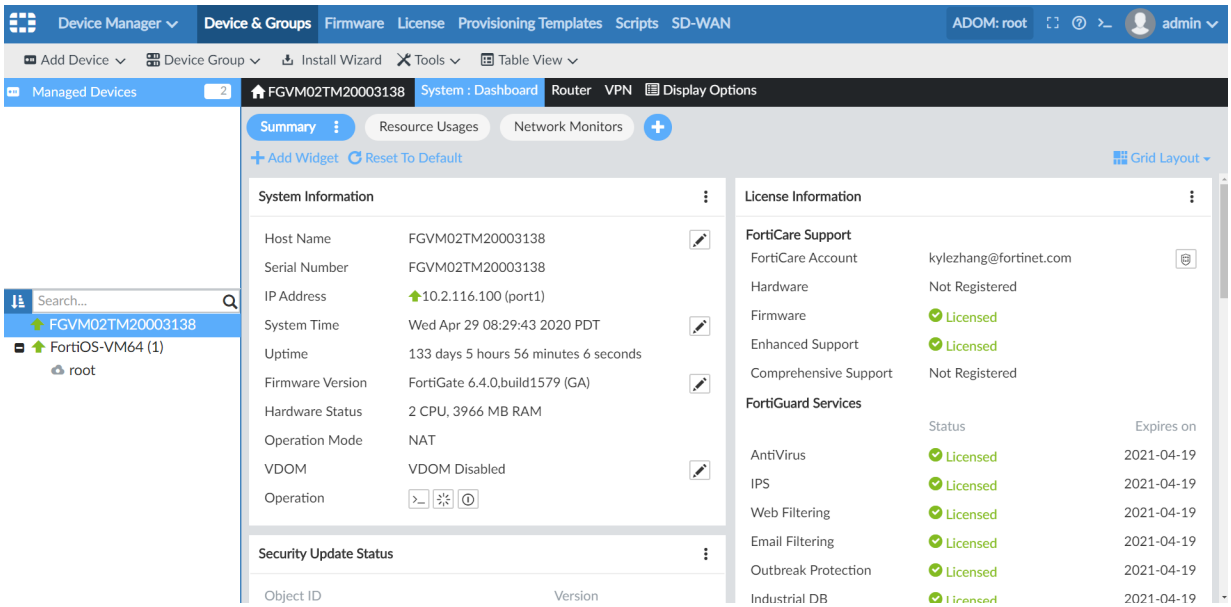
5. Click *Export to PDF* to download the results.

Device Health Monitoring Screen and Widget - 6.4.3

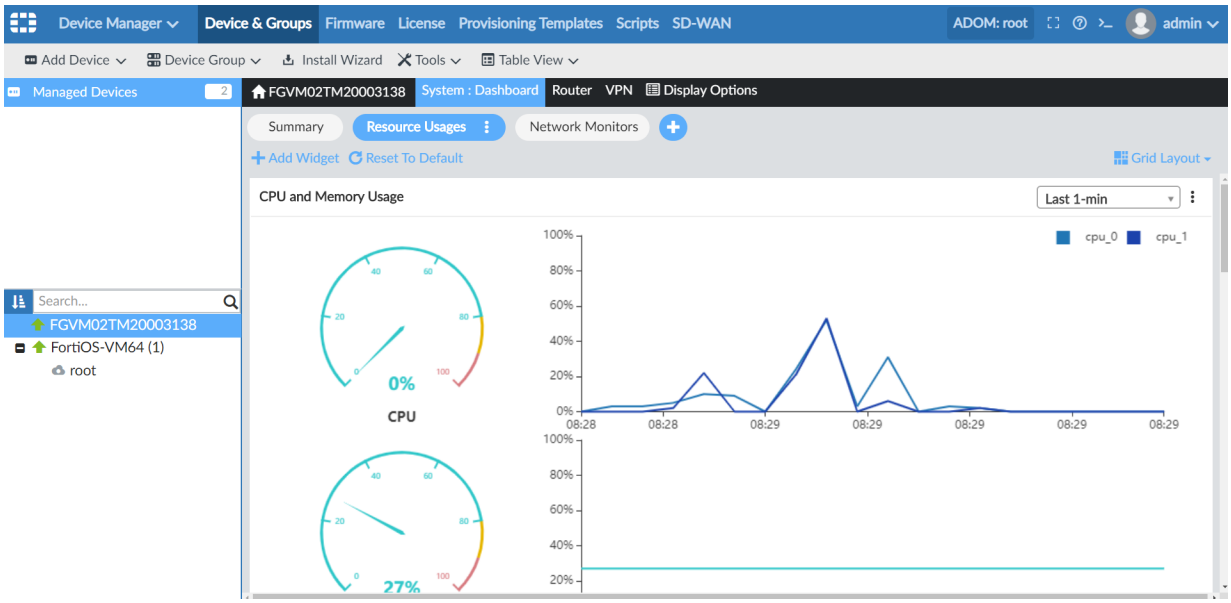
System dashboards and widgets have been enhanced to provide more useful information related to health monitoring, such as DHCP, IPsec VPN, User, and WiFi status.

To add health monitoring dashboards and widgets:

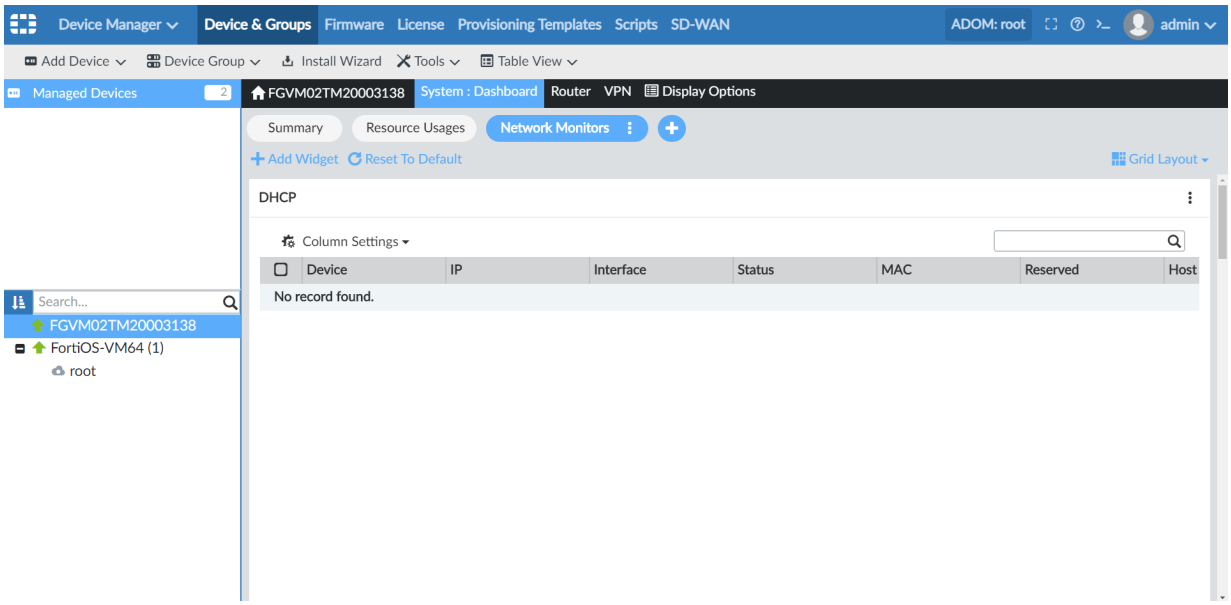
1. Go to *Device Manager* > *Device & Groups*.
2. In the tree menu, select a managed device. The *System: Dashboard* tab displays three dashboards:
   - *Summary*



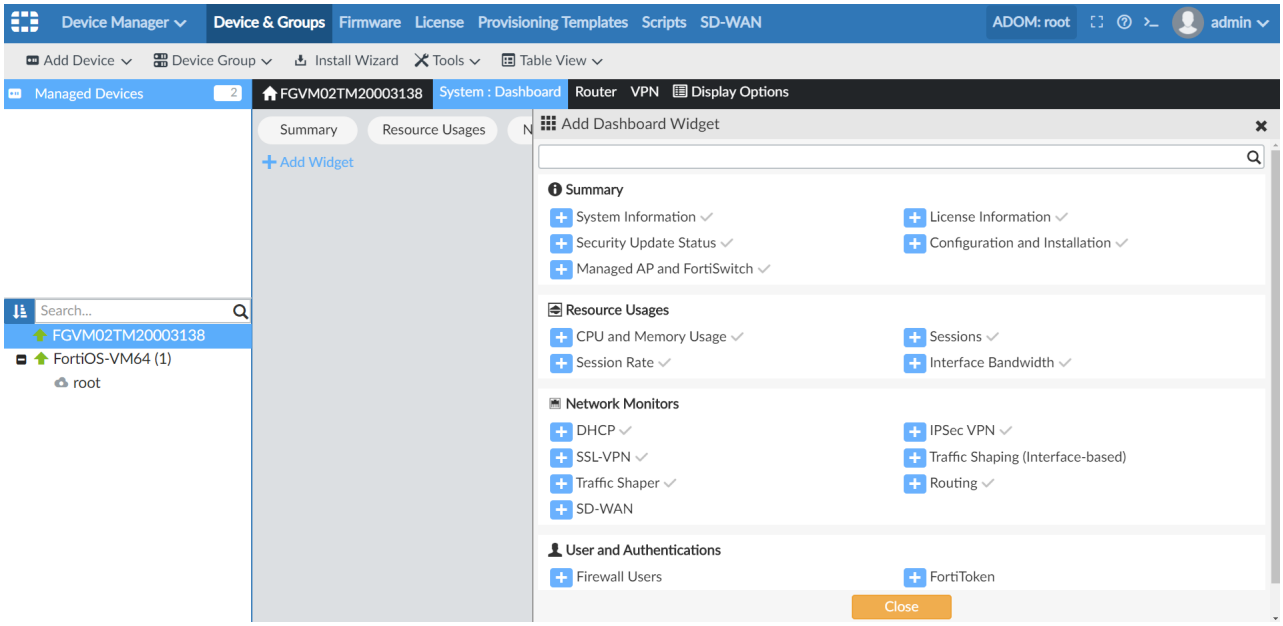
   - *Resource Usage*



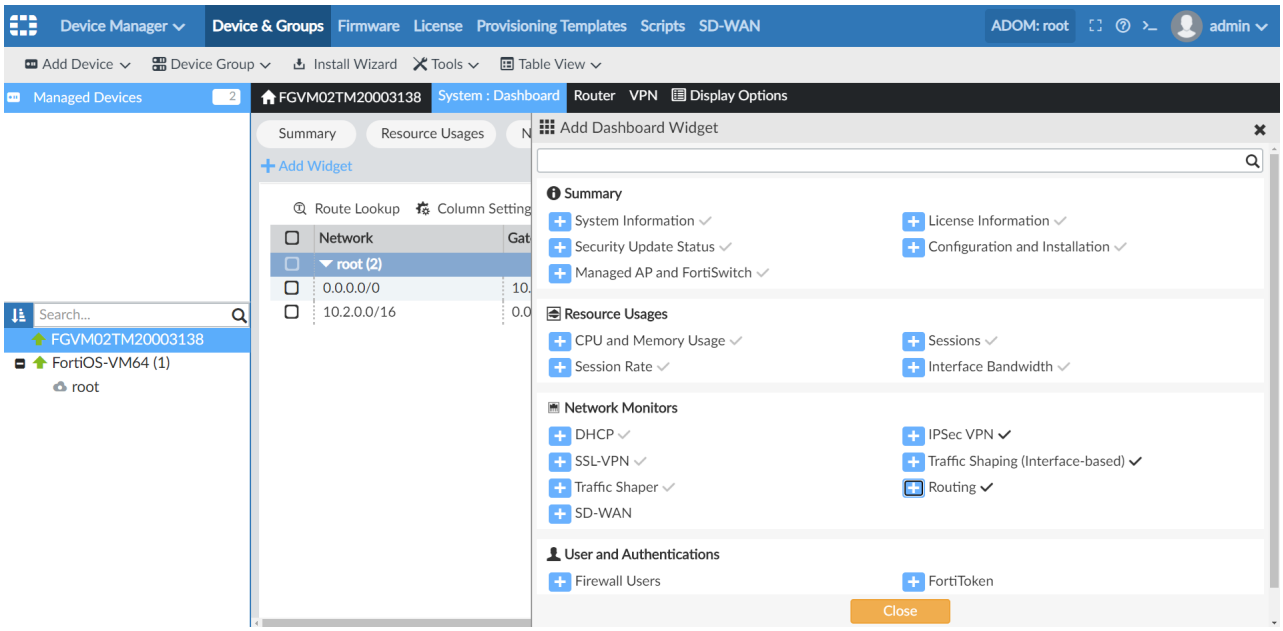
- *Network Monitors*



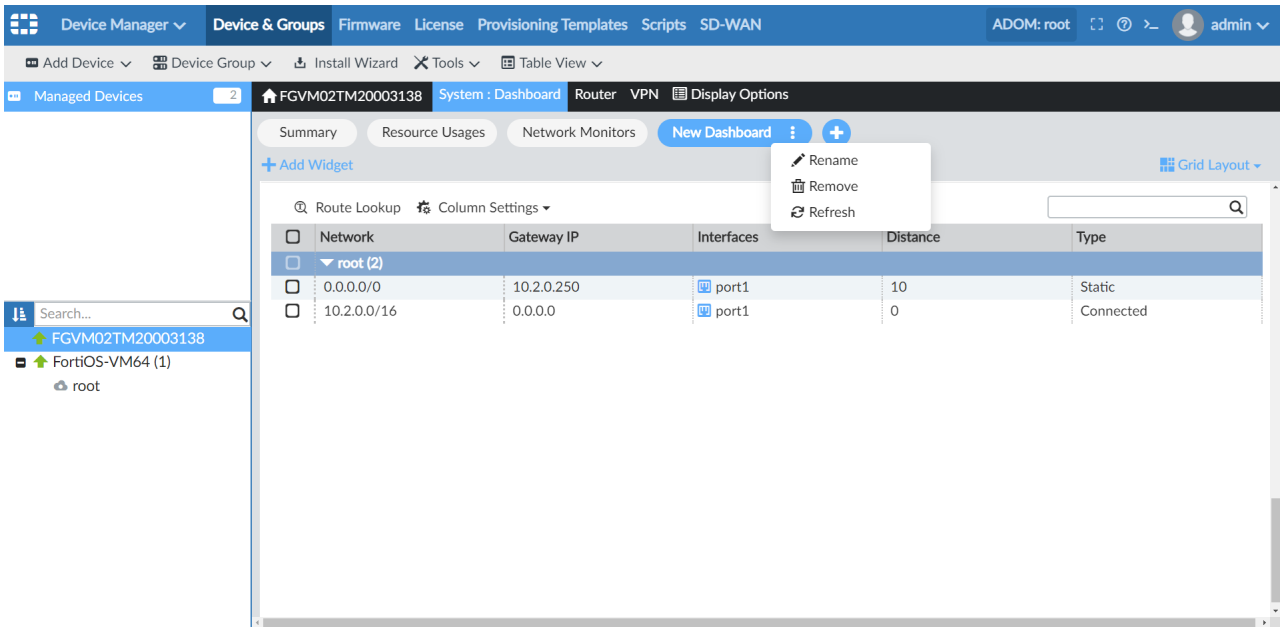
3. Click the (+) icon to add a new dashboard. The *Add Dashboard Widget* dialog is displayed.



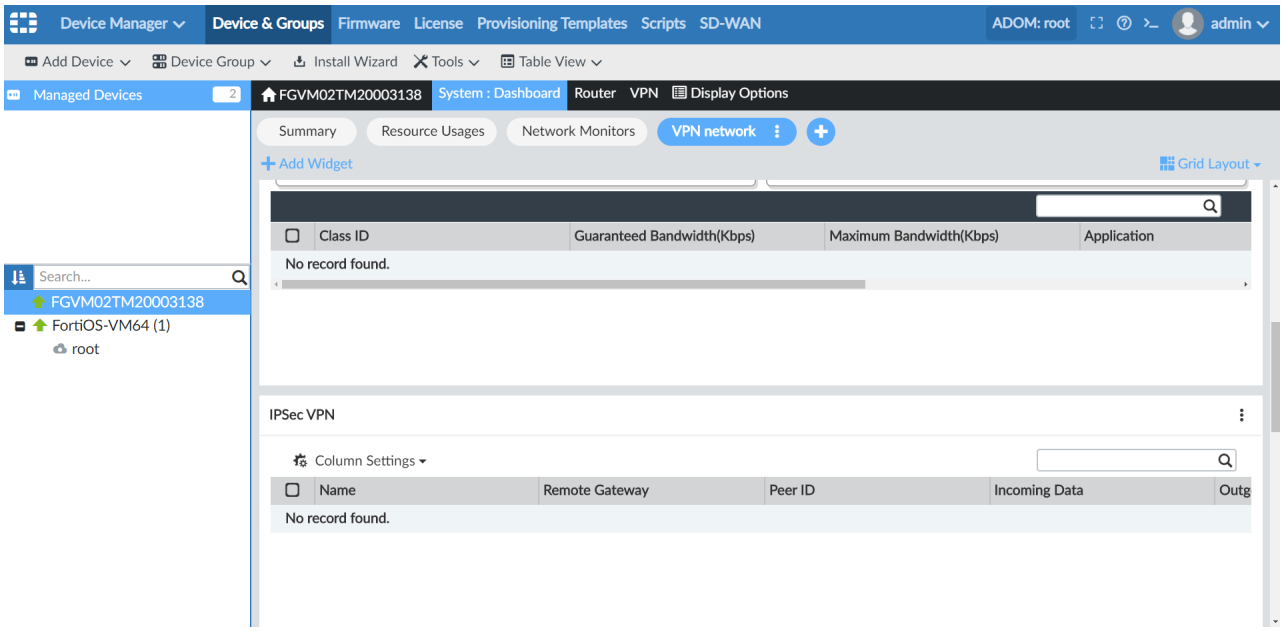
4. Click the add icon (+) to add a widget to the monitor. A checkmark appears next to the widget.



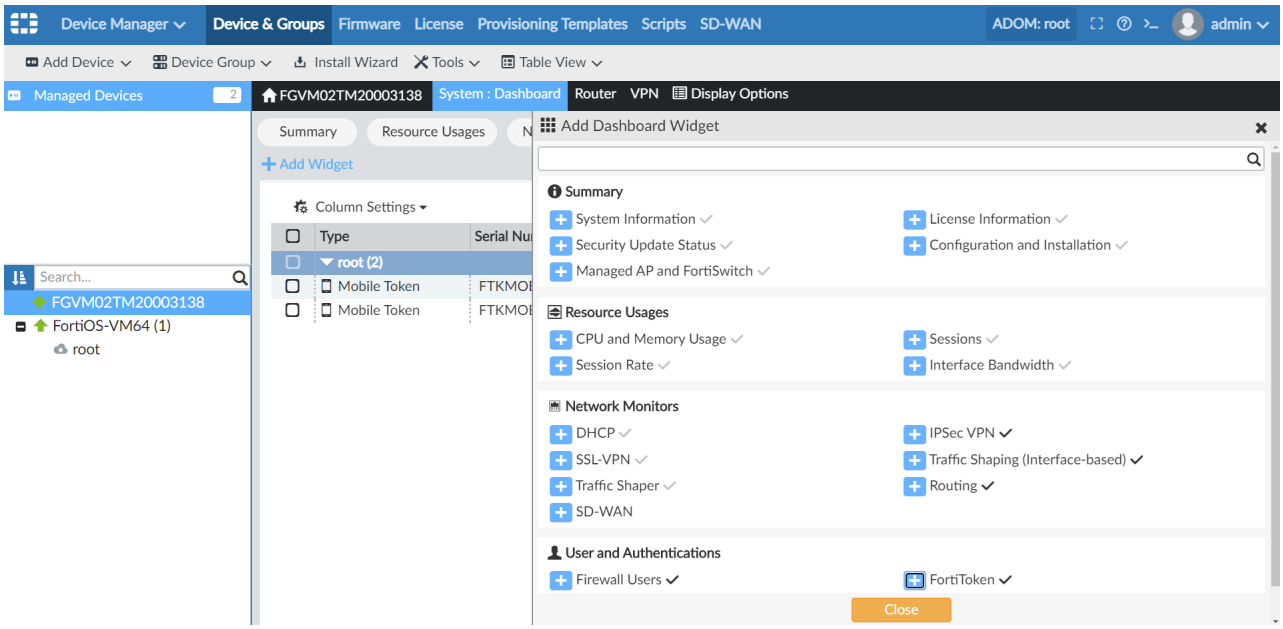
5. Click *Close*. The dashboard is added to the *System: Dashboard* tab.
6. Click the menu icon, and select *Rename* to rename the dashboard.



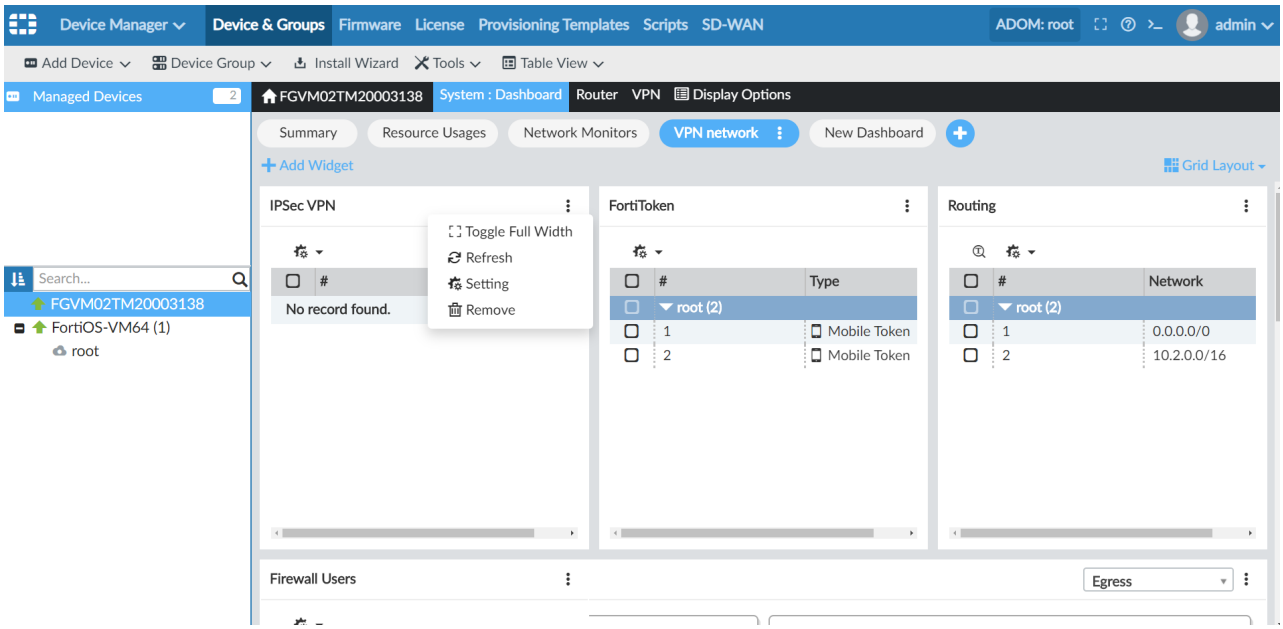
The new name appears above the dashboard.



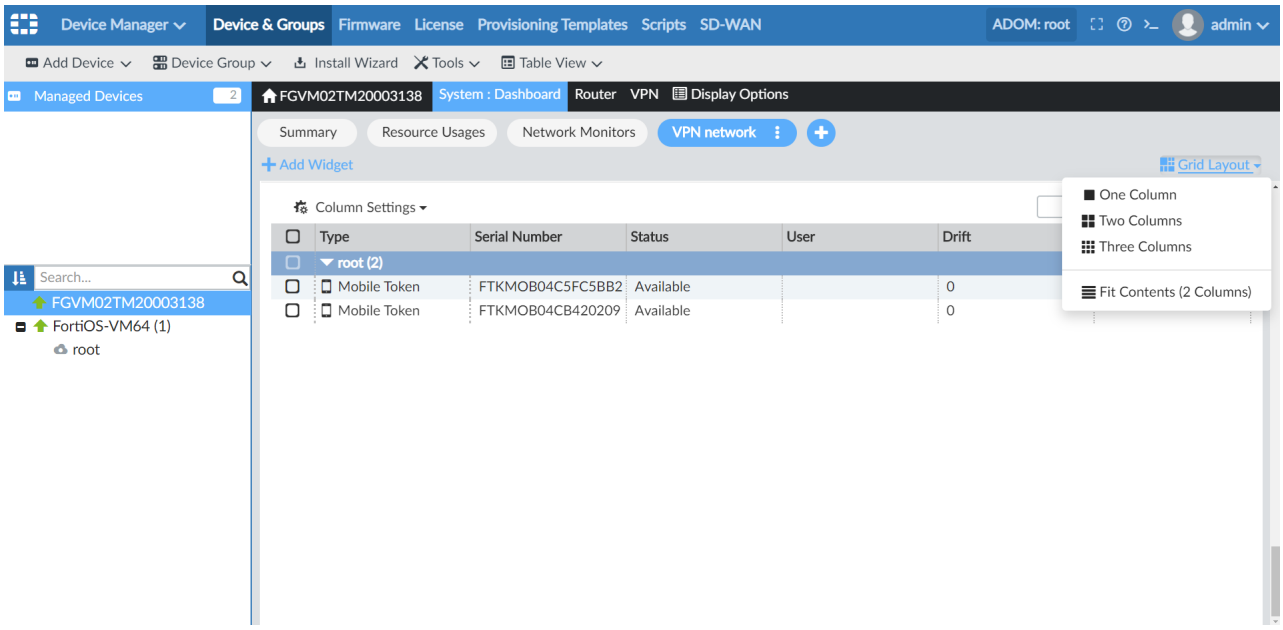
7. Click *Add Widget* to add more widgets to a dashboard.



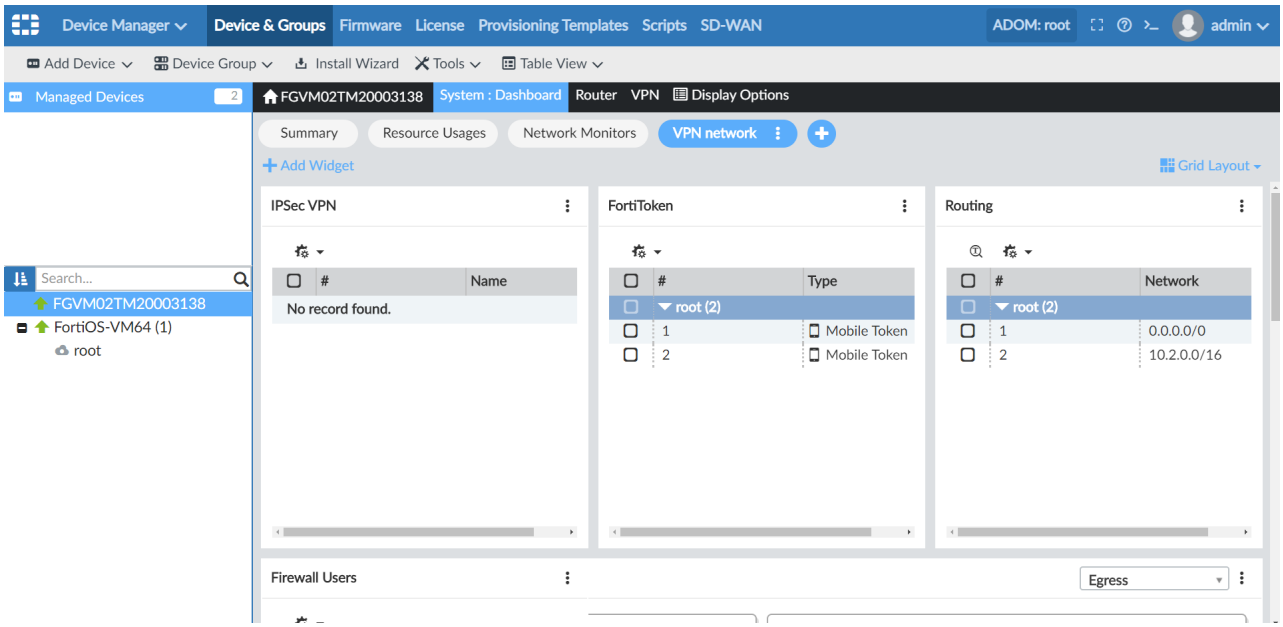
8. Click the menu icon, and select *Remove* to remove a widget from the dashboard.



9. Click *Grid Layout*, and select *Three Columns*.



The widgets are displayed as three columns in the dashboard.



Assign policy packages and system templates during device approval - 6.4.3

When you are authorizing a FortiGate device for central management, you can assign a policy package and a system template as part of the authorization process, and you can override some system template settings.

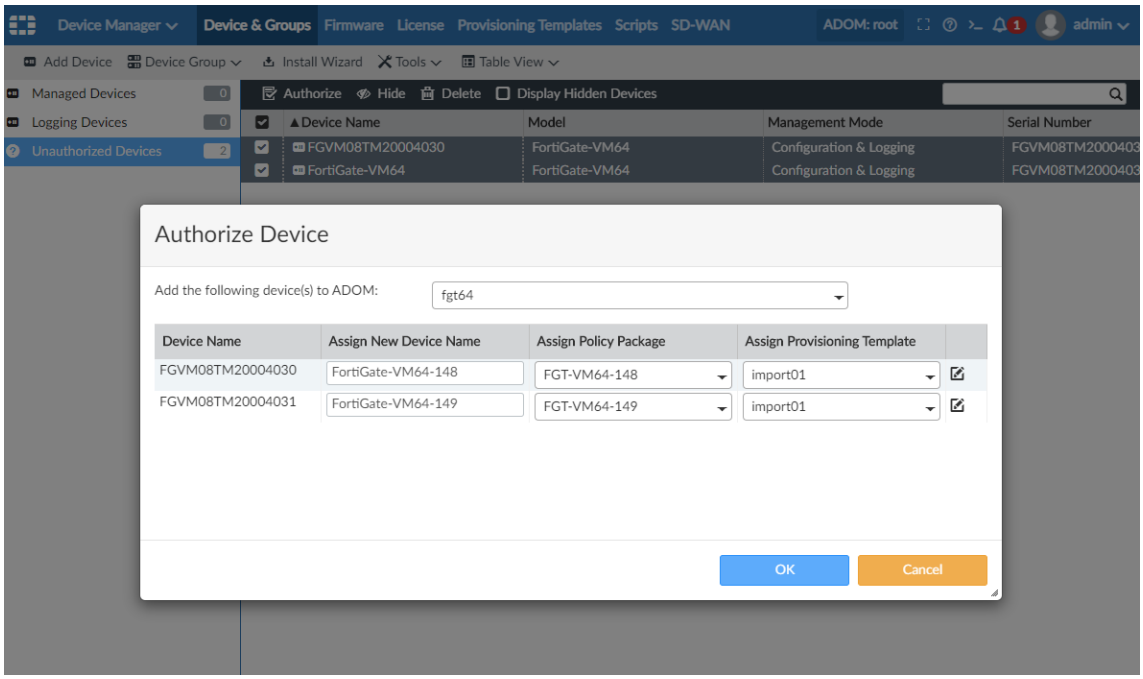
You can specify what settings in a system template can be overridden.

This example describes how to assign a policy package and system template when authorizing a FortiGate for central management. It also describes how to allow and execute overrides in a system template during device authorization.

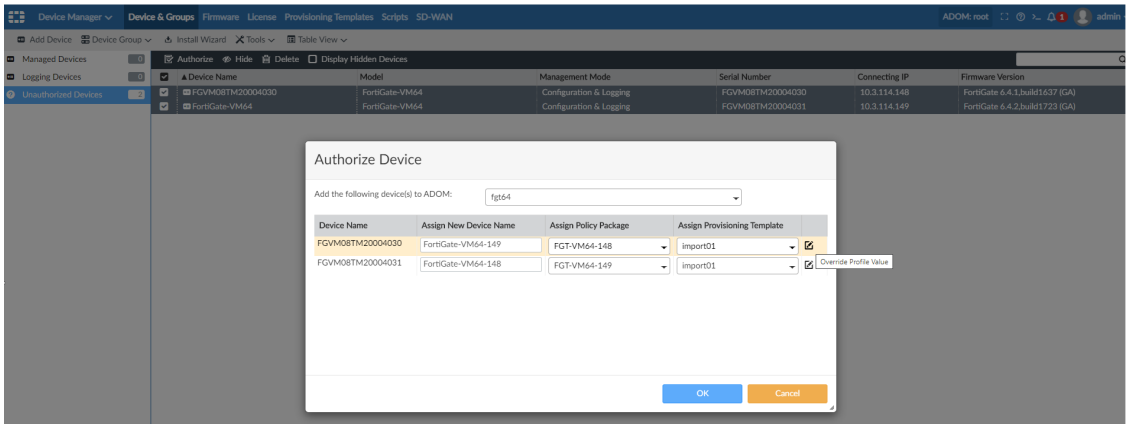
To assign policy packages and system templates during device authorization:

1. In FortiOS, ensure that central management is enabled, and FortiManager is selected.
   These settings allow FortiGate to appear in FortiManager as an unauthorized device.
2. In FortiManager, ensure that you have created the policy packages and system templates that you want to assign to unauthorized devices.
3. In system templates, ensure that you have specified what overrides are allowed.
   a. Go to *Device Manager* > *Provisioning Templates*.
   b. Under *System Templates*, select the system template to open it for editing.
   c. Select the *Allow Override* checkbox beside settings for which you want to allow overrides, and click *Apply*.
   For example, you can allow overrides of settings in the *DNS* widget and in the *Interface* widget.
4. In FortiManager, go to *Device Manager* > *Device & Groups* > *Unauthorized Devices*.
   The list of unauthorized FortiGate devices is displayed.

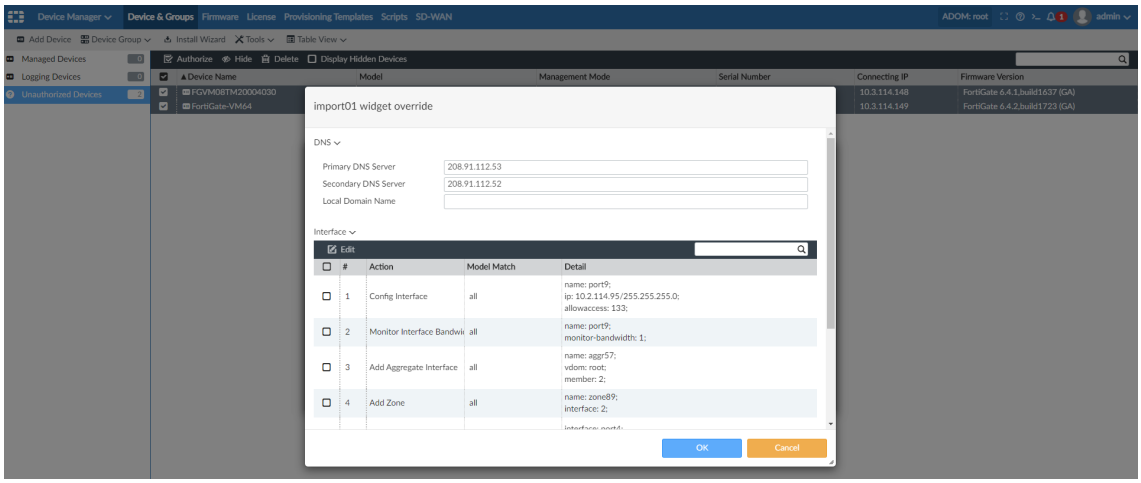
5. Select the unauthorized devices, and click *Authorize*.
   The *Authorize Device* dialog box is displayed.



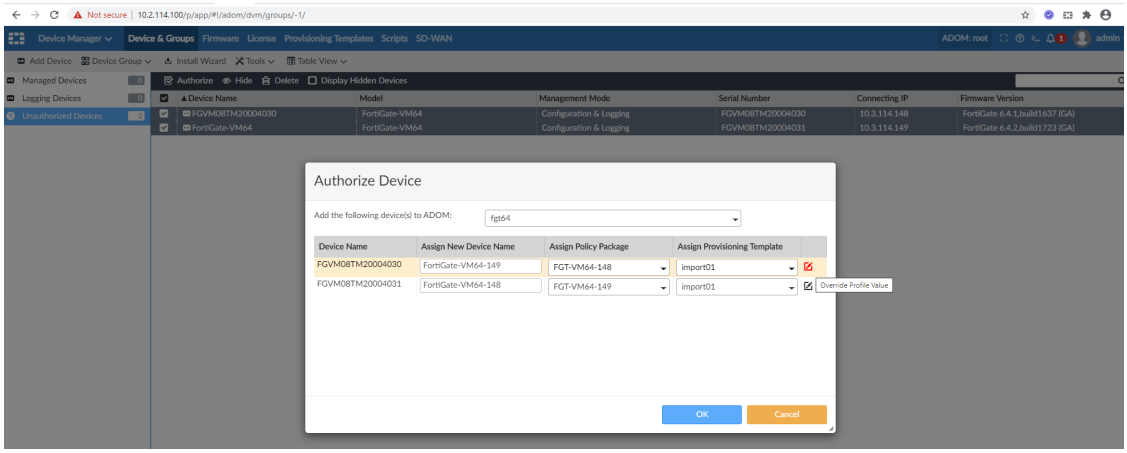
6. In the *Assign Policy Package* list, select a policy package.
7. In the *Assign Provisioning Template* list, select a system template, and click the *Override Profile Value* button.



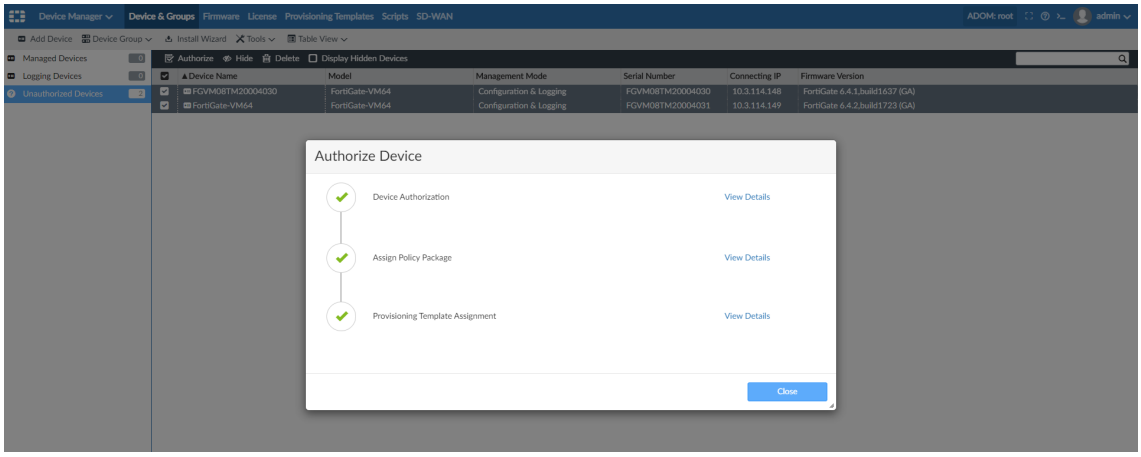
The system template is displayed.



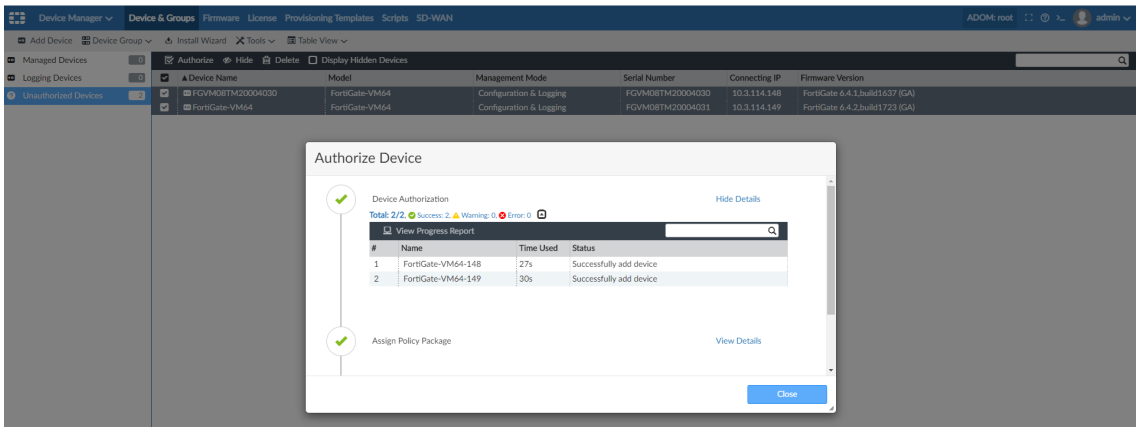
8. Override the editable settings, and click *OK*.
   For example, change the interface settings. The settings are saved, and the *Override Profile Value* button turns red to indicate values have been overridden.



9. Click *OK*.
   Device authorization begins, and you can view details for each step in the process.

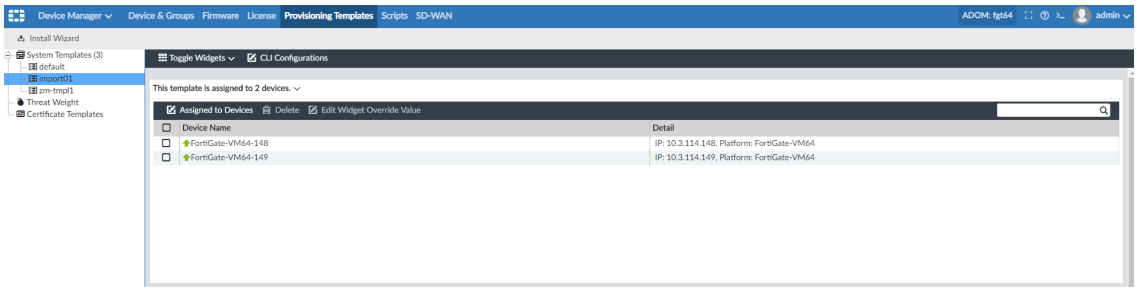


You can click *View Details* to display more details about each step.

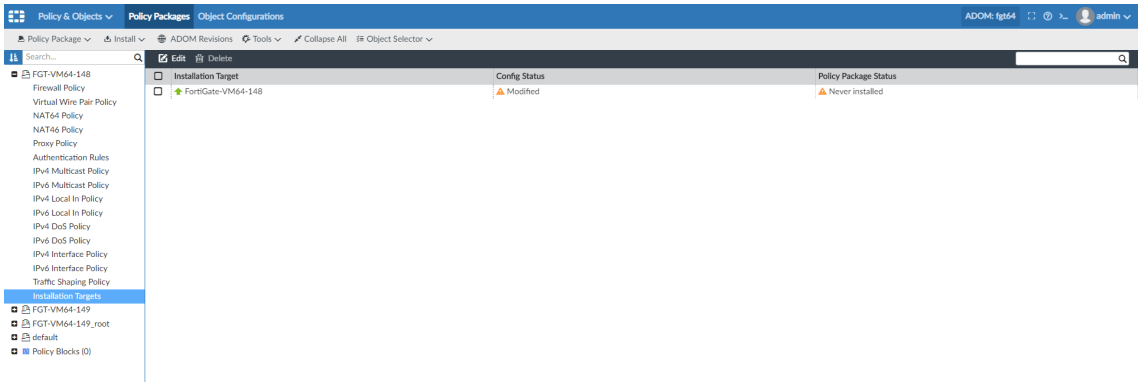


The device is authorized.

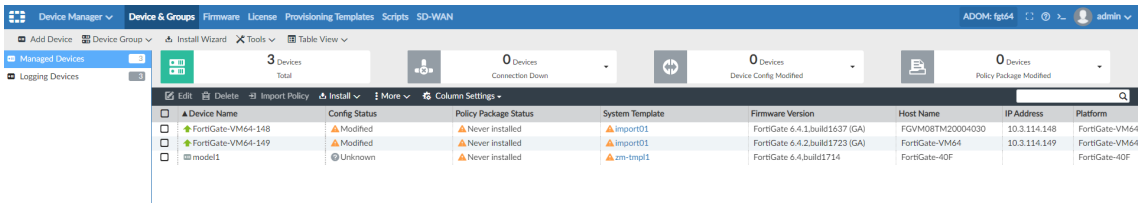
10. Check that the provisioning template is assigned to the authorized device.
    a. Go to *Provisioning Templates* > *System Templates*, and select the template.
    The list of devices to which the template is assigned is displayed.



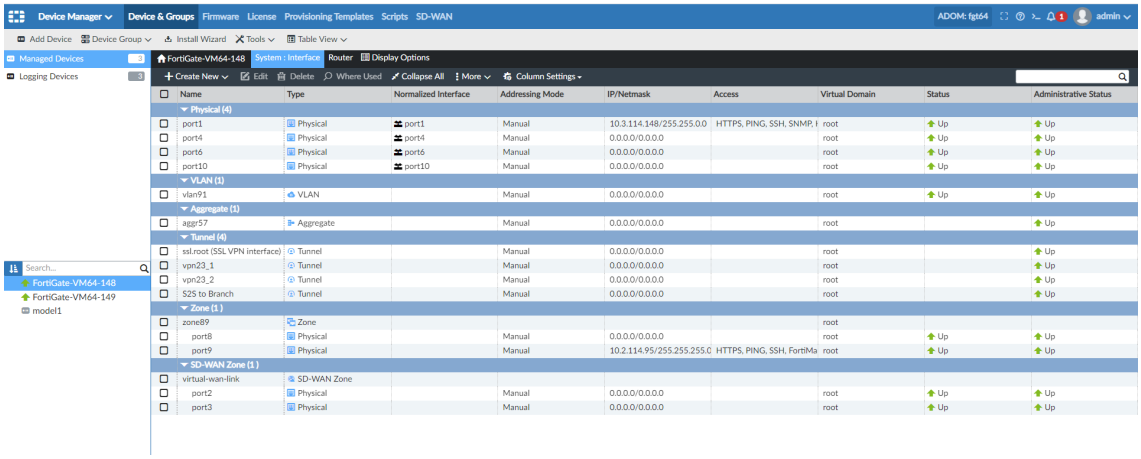
11. Check that the installation target for the policy package lists the authorized device.
    a. Go to *Policy & Object* > *Policy Packages*, and expand the policy package you selected.
    b. Inside the policy package, select *Installation Targets*.
    The list of target devices for the policy package is displayed.



12. Go to *Device Manager* > *Device & Groups* > *Managed Devices*.
    The authorized device is displayed. The *Config Status* is *Modified*, and a configuration installation is needed. Until the configuration is installed, the system interface displays the result of the interface template.



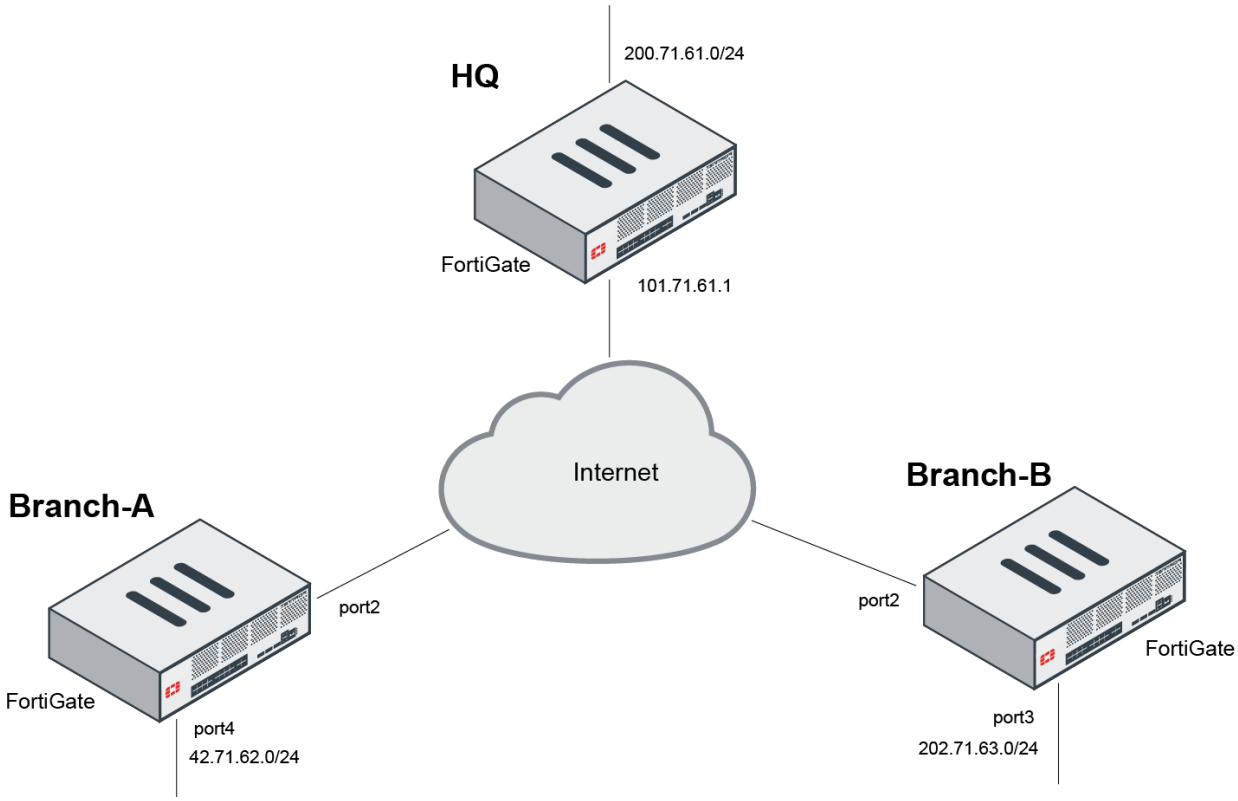
13. Install the configuration to the authorized device.
    The config installation completes.
14. In the lower tree menu, select the device, and go to *System:Interface*.
    The setting from the override is displayed.



IPsec VPN template - 6.4.3

With this feature, you can provision IPsec tunnels to FortiGate branch devices using an IPsec template. You can save an IPsec VPN configuration, apply it to one or more FortiGates, or reuse the same configuration over and over again. You can specifically name IPsec tunnel interfaces using supported meta fields, and the tunnel interfaces may later on be mapped to normalized interfaces, or used in policies and also in SD-WAN widgets.

The following example assumes that site *HQ* IPsec VPN has been configured and is up and running. We will establish the configurations of *Branch-A* and *Branch-B* sites to the *HQ* site by using an IPsec template.



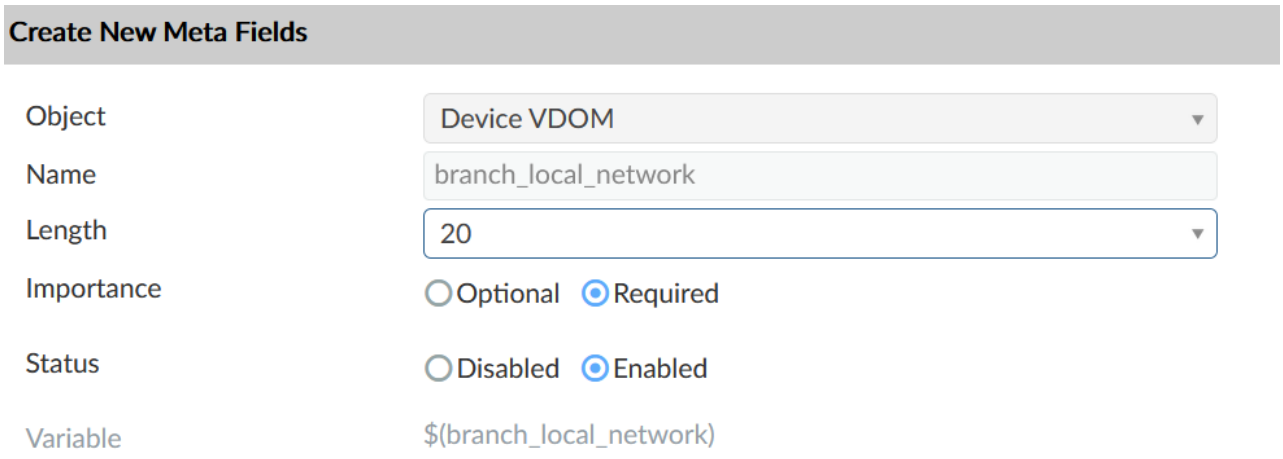
This section describes the following:

Creating new meta fields

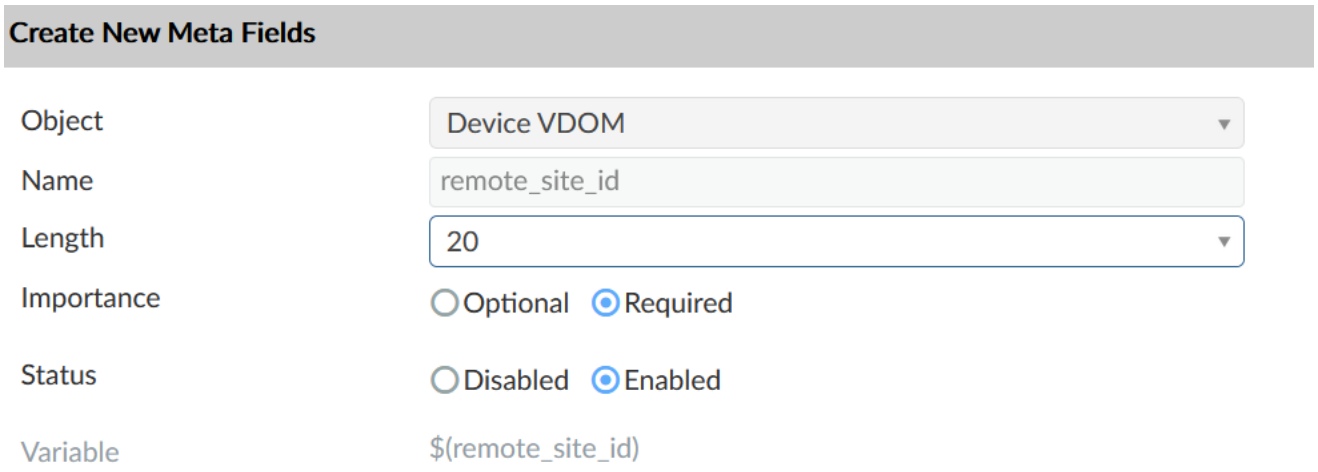
To create a new meta field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Click *Create New* from the toolbar. The *Create New Meta Fields* pane appears.
3. Select the *Object* type from the drop-down list, for example, *Device VDOM*.
4. Enter a value in the *Name* field to name the meta field. The value entered here (`branch_local_network`) becomes the variable name and is indicated in the *Variable* field with the value `$(branch_local_network)` at the bottom.
5. Select the appropriate *Length* from the drop-down list.
6. Select the *Importance* as *Required* to make the meta field mandatory.
7. Select the *Status* as *Enabled* to enable the meta field.

8. Click *OK*. The meta field is created.



Similarly, create another meta field `remote_site_id`.



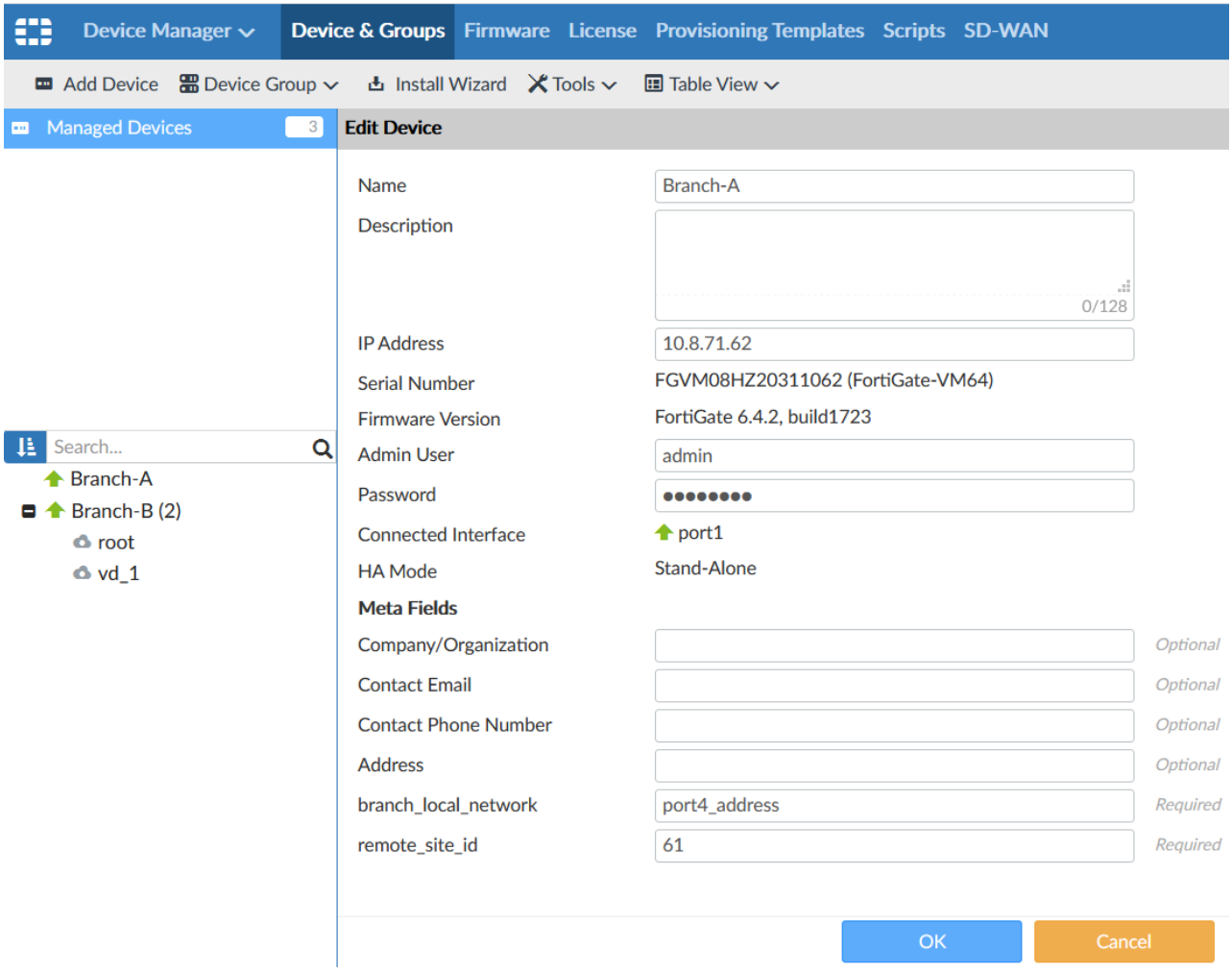
Assigning values to meta field variables

Once meta fields are created, you need to assign values to the meta field variables for each device. You will assign values to the meta field variables `branch_local_network` and `remote_site_id` for both the sites *Branch-A* and *Branch-B*.

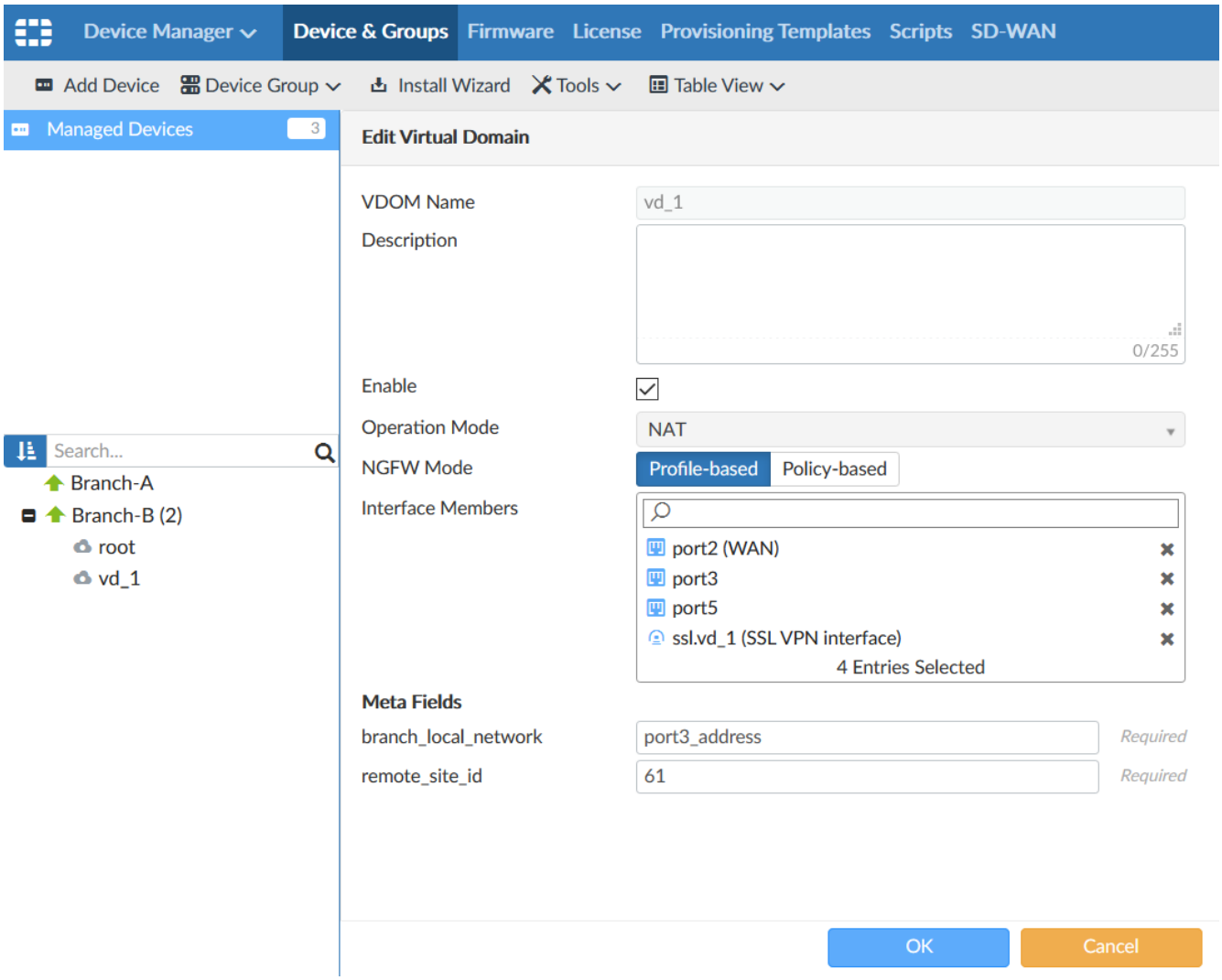
To assign a value to a meta field variable for a device:

1. Go to *Device Manager* > *Device & Groups* > *Managed Devices*.
2. Select device *Branch-A* and click *Edit*. The *Edit Device* pane appears.
3. Scroll down to the *Meta Fields* section and add values for both the *branch_local_network* and *remote_site_id* fields.

4. Click *OK*.



Similarly, edit device *Branch-B* to add values to the meta field variables.



Creating IPsec VPN template

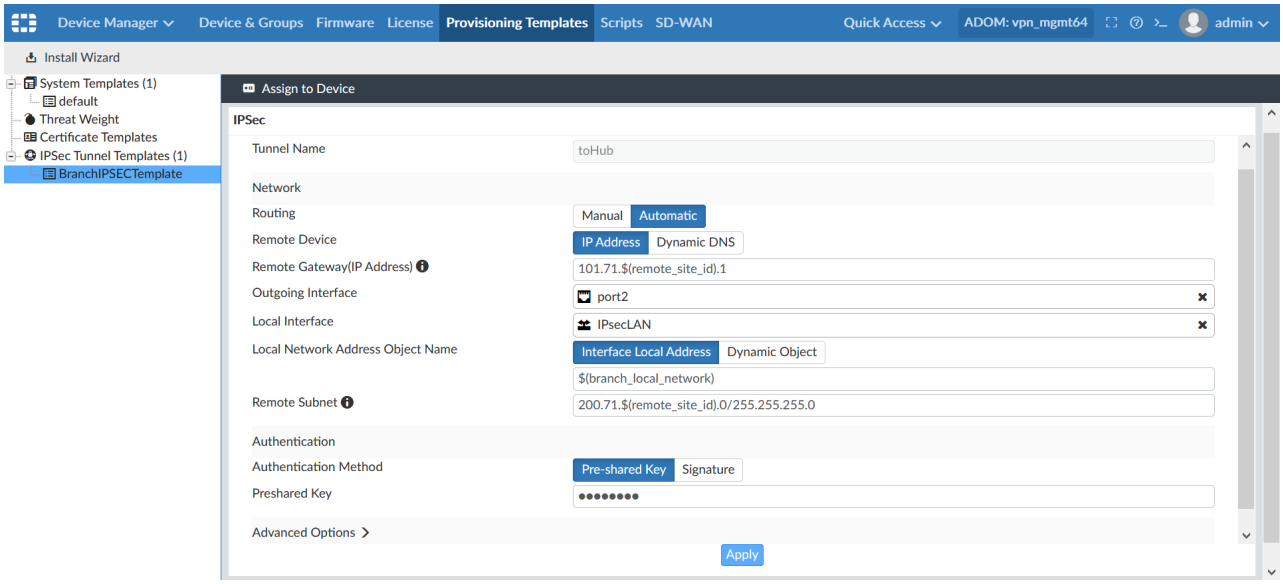
To create an IPsec VPN template:

1. Go to *Device Manager* > *Provisioning Templates* > *IPsec Tunnel Templates*.
2. Click *Create New* from the toolbar. The *Create New IPsec Tunnel Template* dialog appears.
3. Enter a *Name* for the template.
4. Click *OK*. The new template is created.
5. Click on the template name from the tree menu at the left. The *IPsec* settings for the template appear on screen:

Setting	Value/Description
Tunnel Name	Name of the IPsec tunnel.
Routing	*Automatic*: Static routes to remote subnet will be created.
Remote Device	*IP Address*

Setting	Value/Description
Remote Gateway (IP Address)	This field accepts meta field variables and you will use the *remote_site_id* meta field variable here, for example, `101.71.$(remote_site_id).1`, where the meta field variable value will be substituted at runtime.
Outgoing Interface	`port2`
Local Interface	We need to create and select a normalized interface with per-device mapping as different devices use different local interfaces. In this case, it is *IPsecLAN*.
Local Network Address Object Name	Select *Interface Local Address*, and enter the meta field variable `$(branch_local_network)`, where the meta field variable value will be substituted at runtime.
Remote Subnet	Enter `200.71.$(remote_site_id).0/255.255.255.0`, where the meta field variable value will be substituted at runtime.
Authentication Method	*Pre-shared Key*: Alphanumeric key used for device authentication.

6. Click *Apply* at the bottom to save the settings. The IPsec template is created and is ready to be assigned to devices.

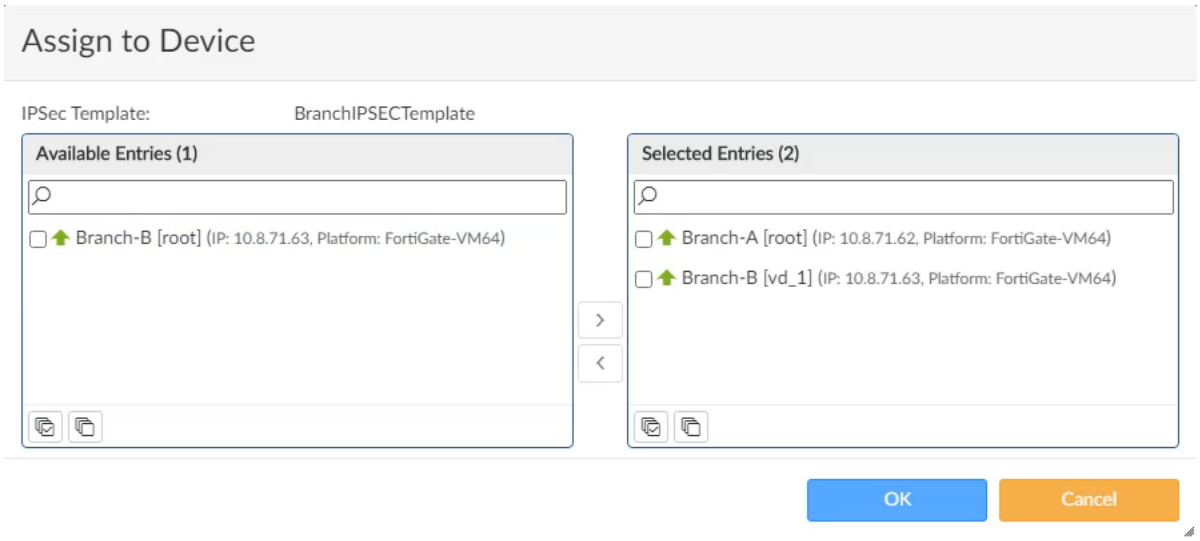


Assigning IPsec VPN template to devices

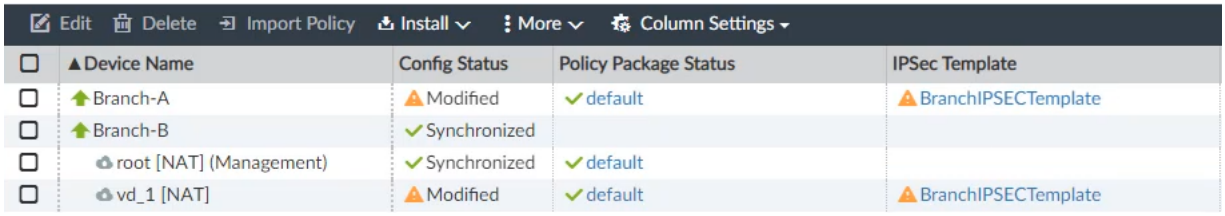
The created IPsec template needs to be assigned to the *Branch-A* and *Branch-B* devices.

To assign an IPsec VPN template to a device:

1. Go to *Device Manager* > *Provisioning Templates* > *IPsec Tunnel Templates*.
2. Click on the template name from the tree menu at the left. The *IPsec* settings for the template appear on screen.
3. Click *Assign to Device* from the toolbar. The *Assign to Device* dialog appears.
4. Select the devices *Branch-A* and *Branch-B* from the list of devices in the *Available Entries* section, and move them to the *Selected Entries* section.



5. Click *OK*. The IPsec template is assigned to the selected devices.

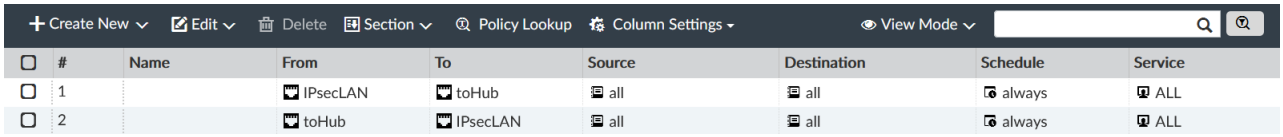


Installing IPsec VPN configuration and firewall policies to devices

Once the IPsec template is assigned to devices, it still does not automatically push the settings to the devices. This is indicated by the *Caution* icon before the template name in the *IPsec Template* column. You need to install the IPsec VPN configuration and firewall policies to those devices for the IPsec template to push through all the settings.

To install IPsec VPN configuration and firewall policies to a device:

1. Go to *Policy & Objects* > *Policy Packages* > *Firewall Policy*.
2. Click *Create New* from the toolbar. The *Create New Firewall Policy* pane appears.
3. Create two firewall policies for traffic between the normalized interface and *HQ* site.

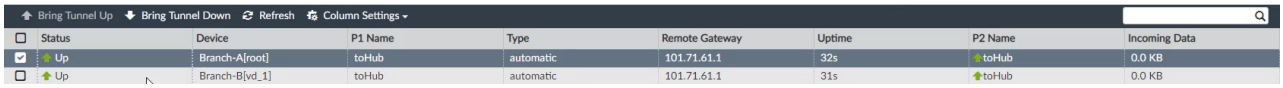


4. Click *Install* > *Install Wizard* from the toolbar. The *Install Wizard* dialog appears.
5. Continue with the policy installation on both *Branch-A* and *Branch-B* devices.
6. Click *Finish*. The firewall policies are installed and the IPsec VPN configurations are pushed to the devices.

Verifying IPsec VPN tunnel status

To verify IPsec VPN tunnel status:

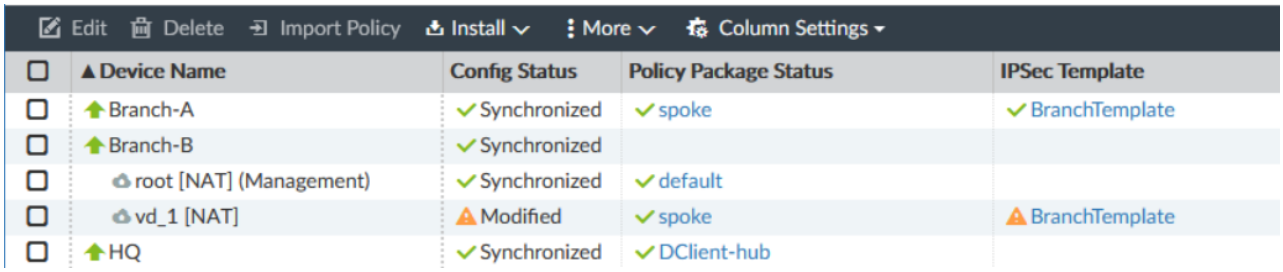
1. Go to *VPN Manager* > *Monitor*.
2. Check the tunnel status from the *Status* column. The tunnels may be *Down*.
3. Select the tunnels with a *Down* status and click *Bring Tunnel Up* from the toolbar.
4. Click *OK* to confirm in the *Bring Tunnel Up* dialog.
5. Click *Refresh* from the toolbar to verify that the tunnels have an updated *Up* status.



Verifying IPsec template configuration status

To verify IPsec template configuration status:

1. Go to *Device Manager* > *Device & Groups* > *Managed Devices*.
2. Click *Column Settings* from the toolbar and select *IPsec Template*. The *IPsec Template* column appears in the table.



A device with a synchronized template status would be indicated by a green tick mark icon before the template name in the *IPsec Template* column, while a device with a modified status would be indicated by a yellow triangle caution icon.

Support FortiSOAR license update in an air-gapped environment (closed network) - 6.4.3

You can now create fabric ADOMs. When you add FortiSOAR devices to FortiManager as unmanaged devices, you can only authorize FortiSOAR devices to fabric ADOMs.

In addition, you can use FortiGuard module in FortiManager in a closed network for license updates to FortiSOAR devices.

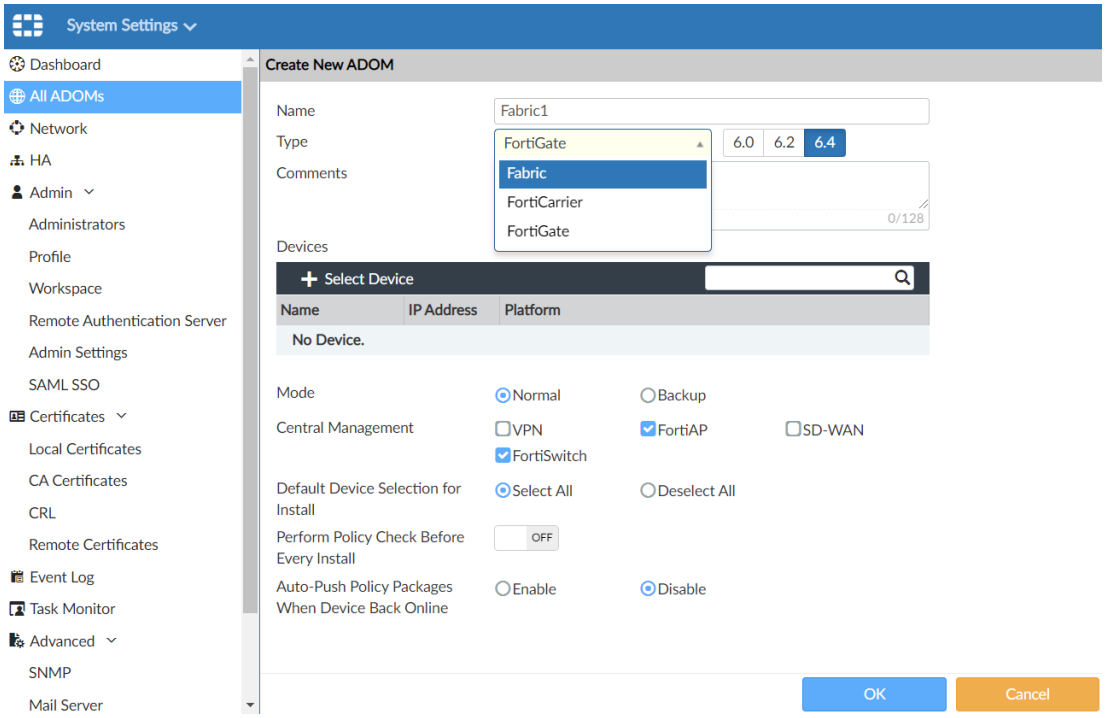
This topic contains the following sections:

Creating ADOMs of type Fabric

You can create ADOMs and select type *Fabric*. You can then select the ADOM when you authorize unmanaged FortiSOAR devices.

To create ADOMs of type Fabric:

1. Ensure that ADOMs are enabled on *System Settings* > *Dashboard*.
2. Go to *System Settings* > *All ADOMs*.
3. Click *Create New*.
   The *Create New ADOM* pane is displayed.
4. In the *Name* box, type a name for the ADOM.
5. In the *Type* list, select *Fabric*.



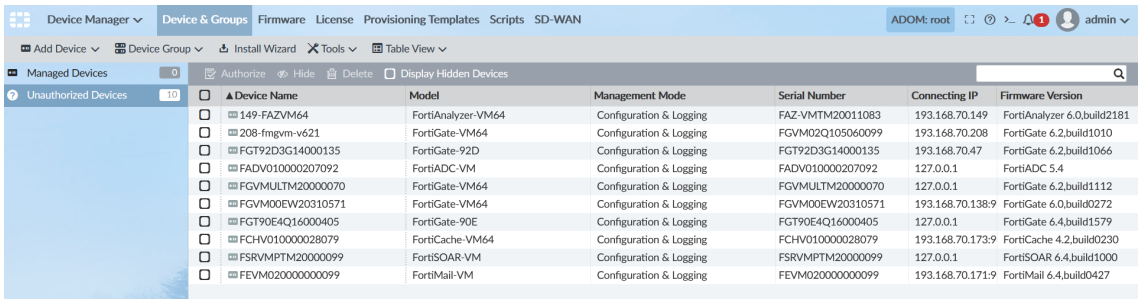
6. Configure the settings for the new ADOM, and click *OK*.
   The new ADOM displays on the *All ADOMs* page in the *Security Fabric*.

Authorizing FortiSOAR devices

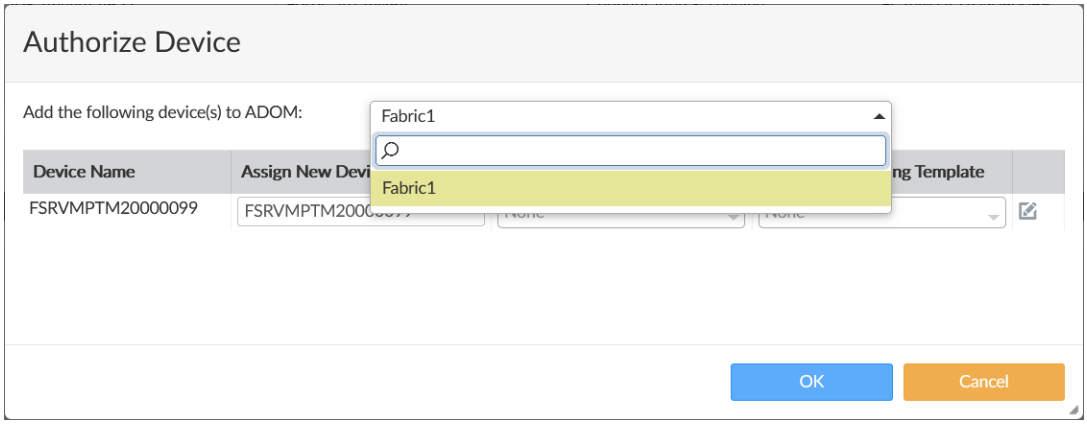
When you authorize FortiSOAR devices, you can only add them to ADOMs of type Fabric. Before you authorize FortiSOAR devices, ensure that you enable ADOMs on FortiManager and create an ADOM of type Fabric.

To authorize FortiSOAR devices:

1. On FortiSOAR, add the FortiManager IP and configured port as the FortiGuard override server.
   FortiSOAR displays in FortiManager as an unauthorized device.
2. In FortiManager, select the *root* ADOM, and go to *Device Manager* > *Device & Groups* > *Unauthorized Devices*.
   FortiSOAR displays as an unauthorized device.



3. Select the FortiSOAR device, and click *Authorize*.
   The *Authorize Device* dialog box displays.
4. In the *Add the following device(s) to ADOM* list, select the fabric ADOM, and click *OK*.



The FortiSOAR device is authorized and displayed in the fabric ADOM.

Updating FortiSOAR licenses in closed networks

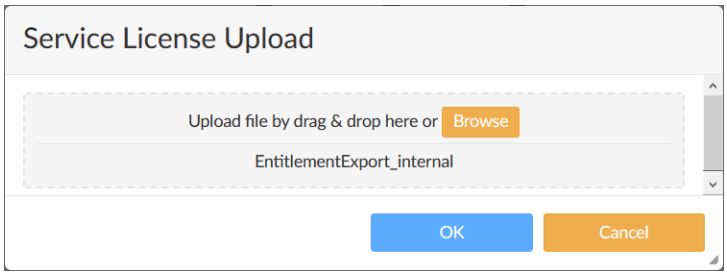
You can use FortiManager in a closed network to update licenses for FortiSOAR devices.

Before you can use FortiManager in a closed network to update licenses for FortiSOAR devices, you must perform the following tasks:

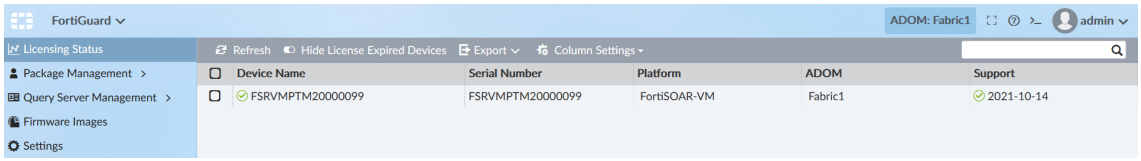
- Add FortiSOAR devices to FortiManager as unmanaged devices, and authorize FortiSOAR devices to a fabric ADOM.
- Request the entitlement file for FortiSOAR devices from the Fortinet Customer Service & Support site

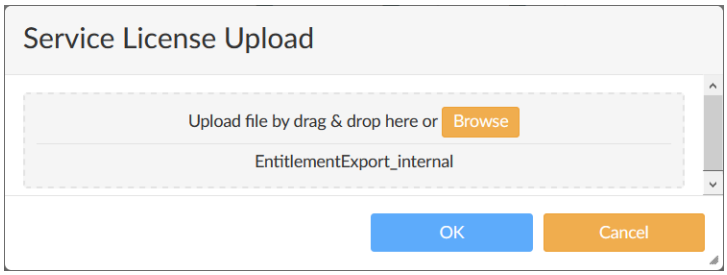
To update FortiSOAR licenses in closed networks:

1. In FortiManager, go to *FortiGuard* > *Settings*, and ensure that *Enable Communication with FortiGuard Server* is toggled *OFF*.
   test
2. Under *Upload Options for FortiGate/FortiMail*, click *Upload* beside *Service License*.
   Although the option is labeled for FortiGate or FortiMail, you can use this option for other types of devices, such as FortiSOAR.
   The *Service License Upload* dialog box is displayed.



3. Drop the account entitlement file on the dialog box, and click *OK*.
   The license information is uploaded.
4. Go to *Licensing Status* to view licensing information for FortiSOAR.





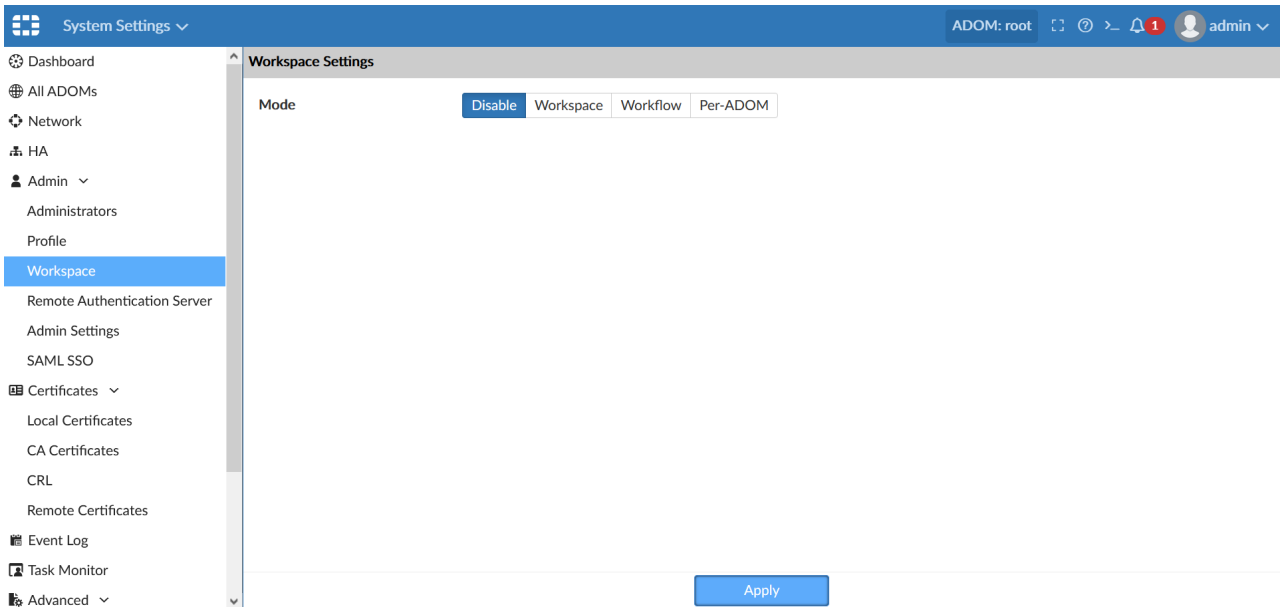
Workspace Mode can be set per-ADOM - 6.4.3

Workspace mode can be configured on a per-ADOM basis.

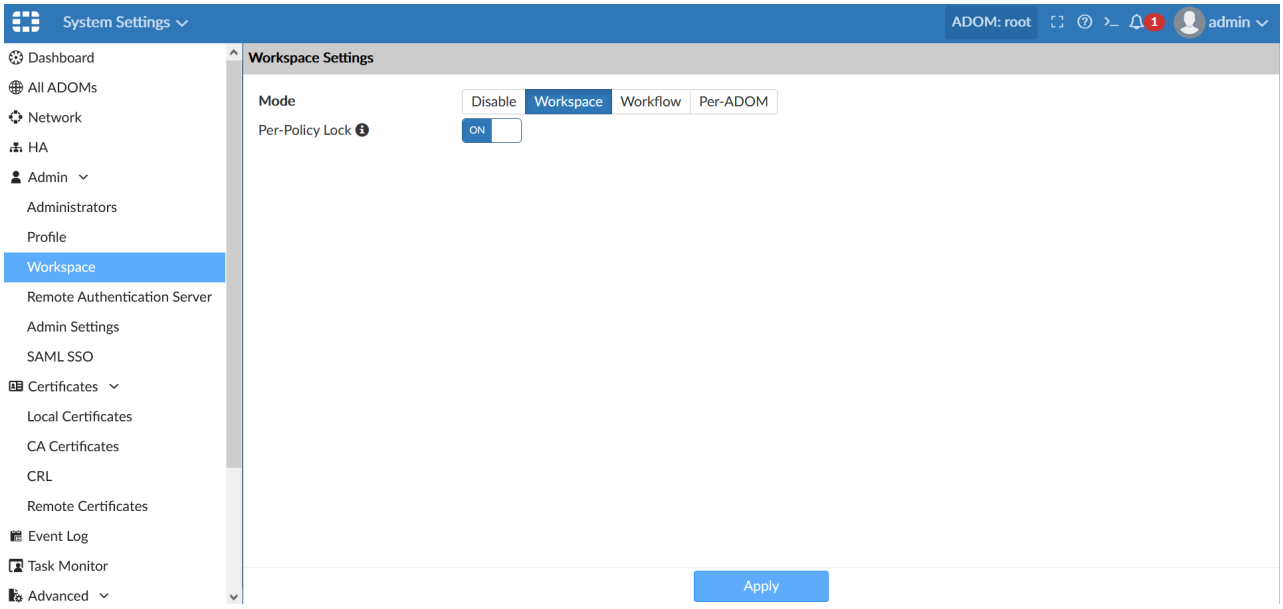
Each ADOM can be individually set to a different workspace mode. For example, the root ADOM can be set to default mode, ADOM 1 can be set to *Workspace* mode, and ADOM 2 can be set to *Workflow* mode.

To enable global workspace mode settings:

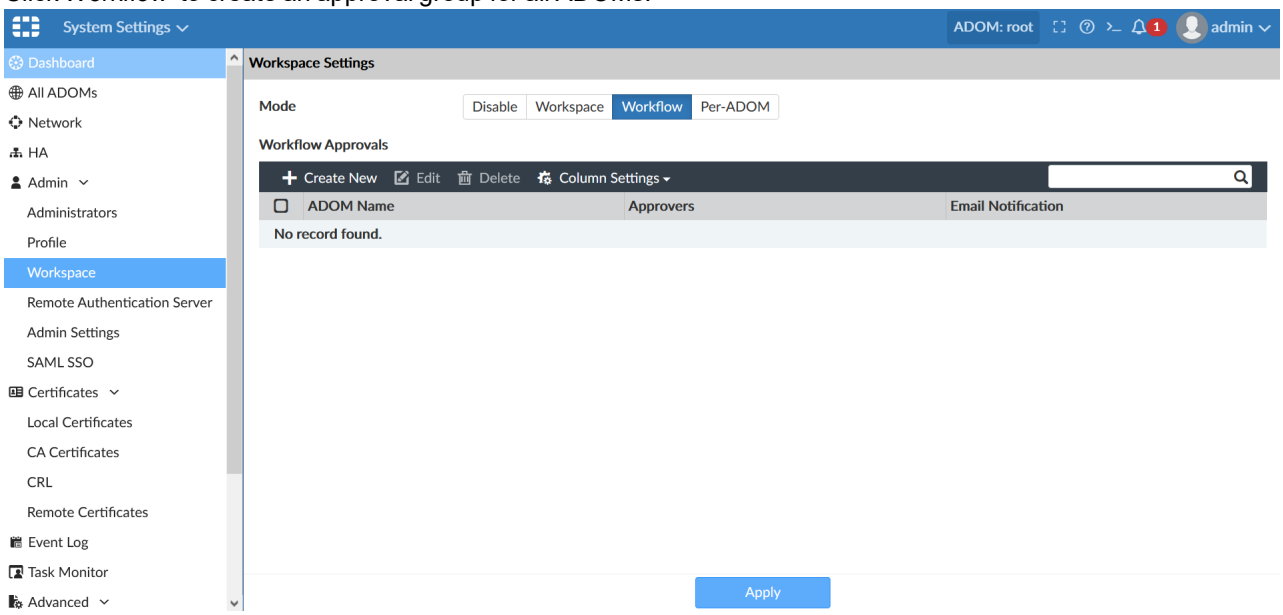
1. Go to *System Settings* > *Admin* > *Workspace*.
   Disable, *Workspace*, or *Workflow* are global workspace settings.



2. Click *Workspace* to enable the setting on all ADOMs.

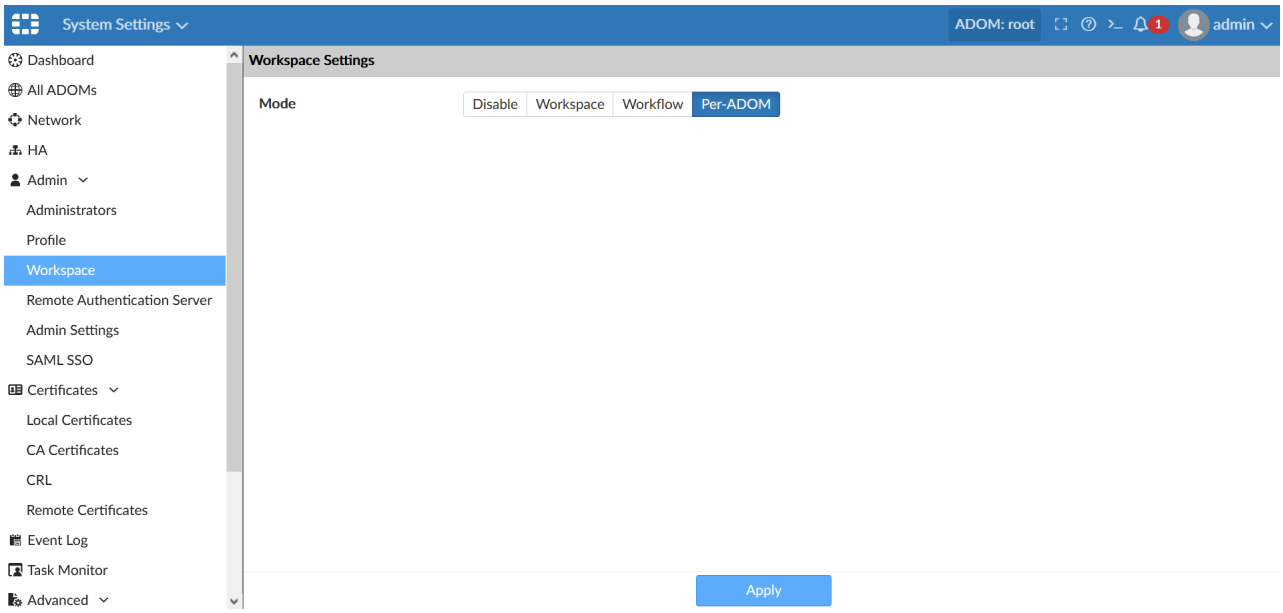


Click *Workflow* to create an approval group for all ADOMs.



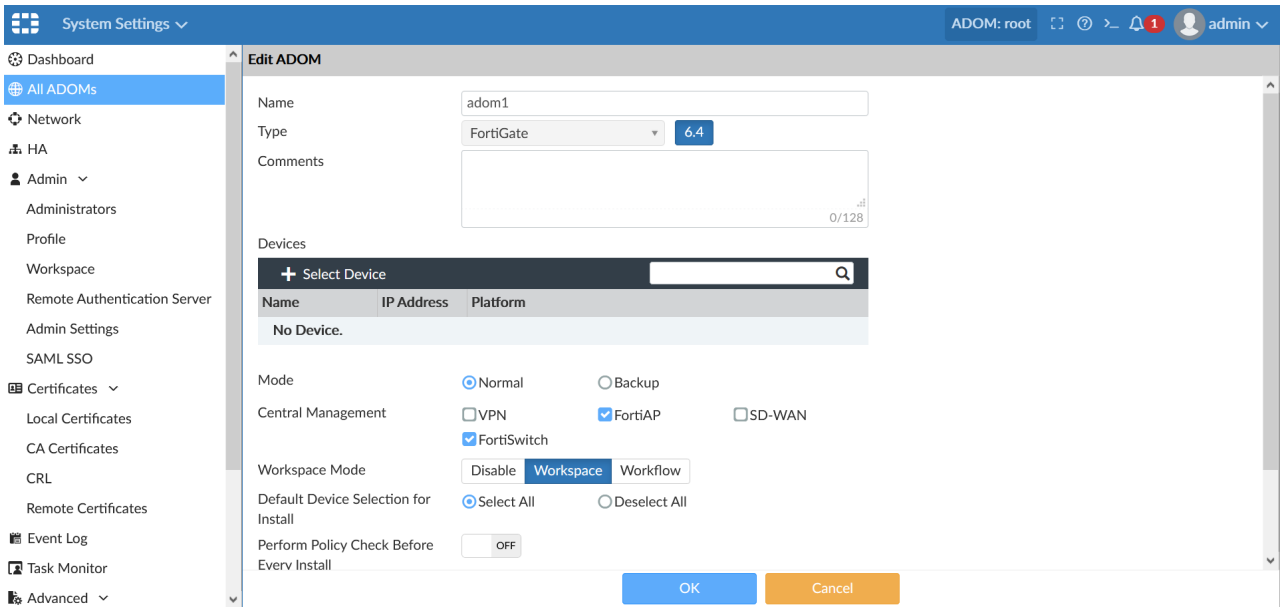
To enable workspace mode per-ADOM:

1. Go to System *Settings* > *Admin* > *Workspace*, and click *Per-ADOM*.

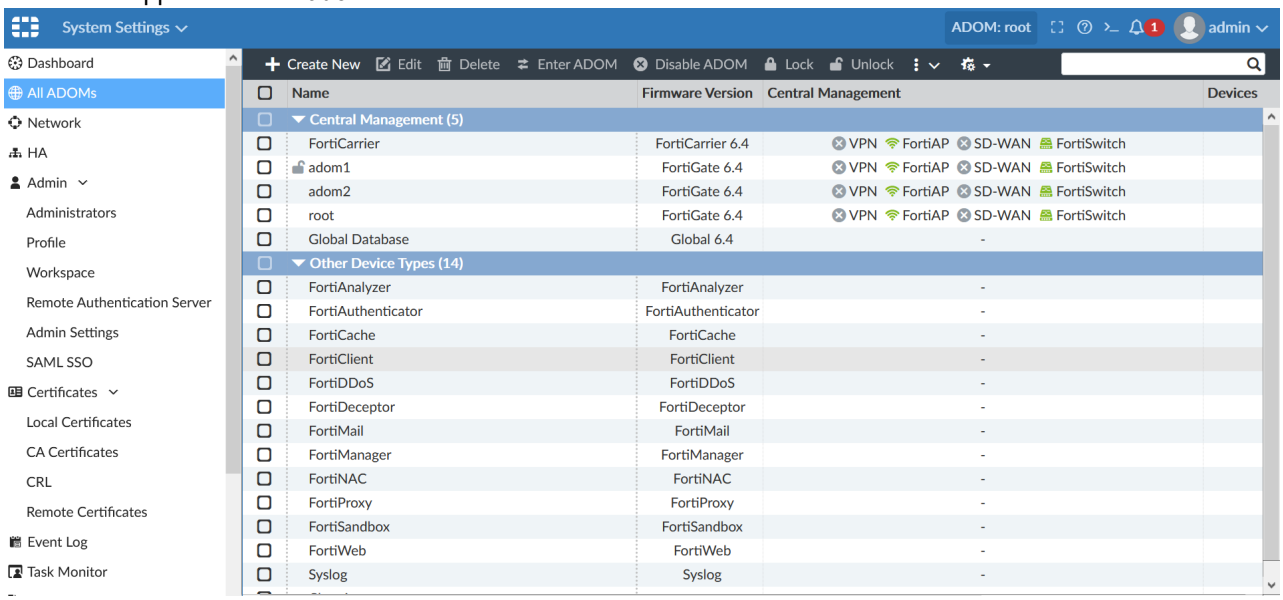


2. Go to *System Settings* > *All ADOMs*.

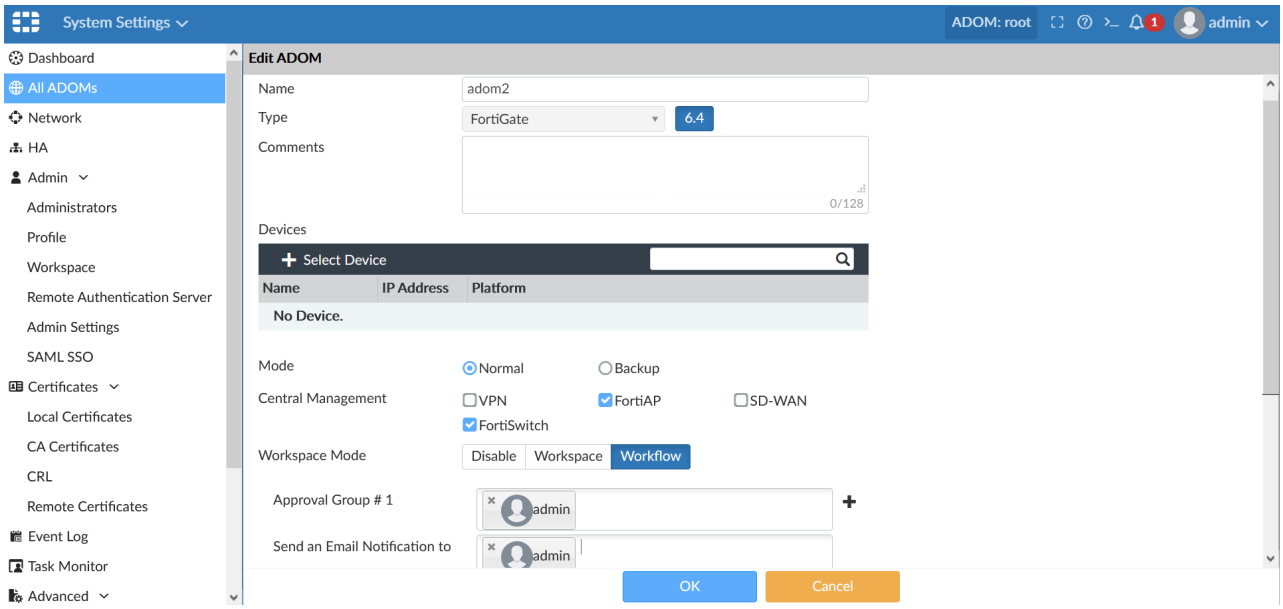
3. Double-click *adom1* to edit it. Click *Workspace*,and then click *OK*.



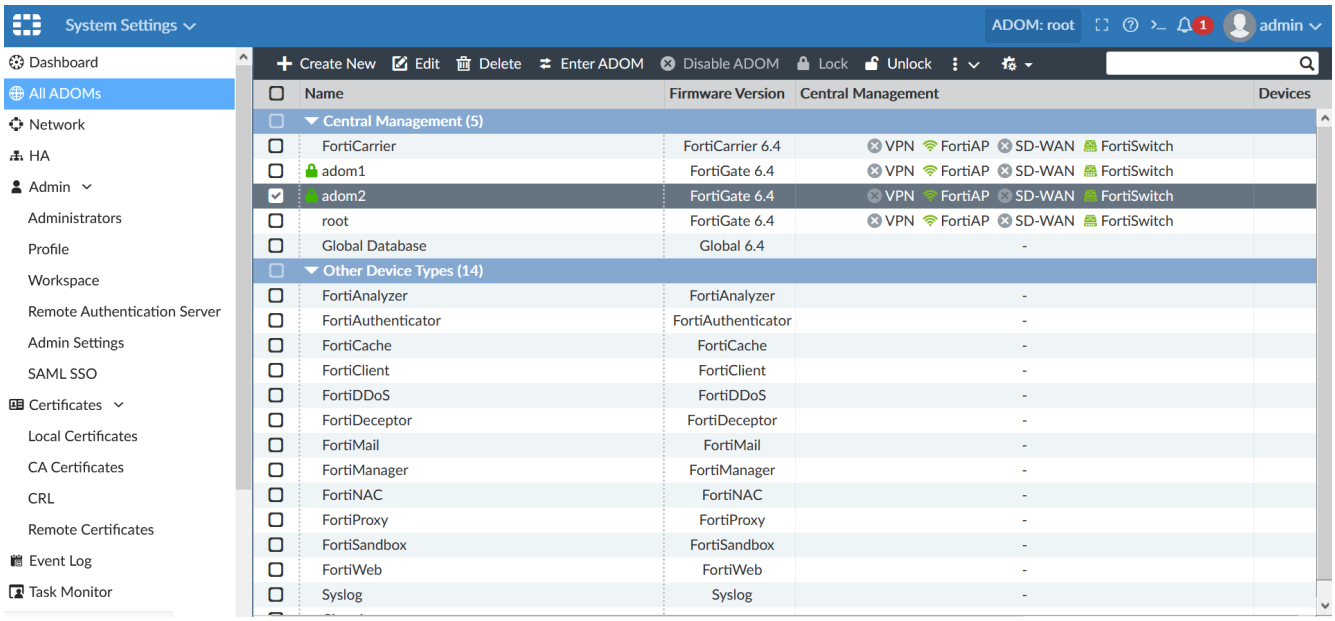
A lock icon appears next to *adom1*.



4. Double-click *adom2*. Click *Workflow*, configure the approval group for this ADOM, and then click *OK*.



The *root* ADOM is now set to default mode, *adom1* is set to *Workspace* mode, and *adom2* is set to *Workflow* mode. To make changes to *adom1* and *adom2*, the admin must lock the ADOM first.



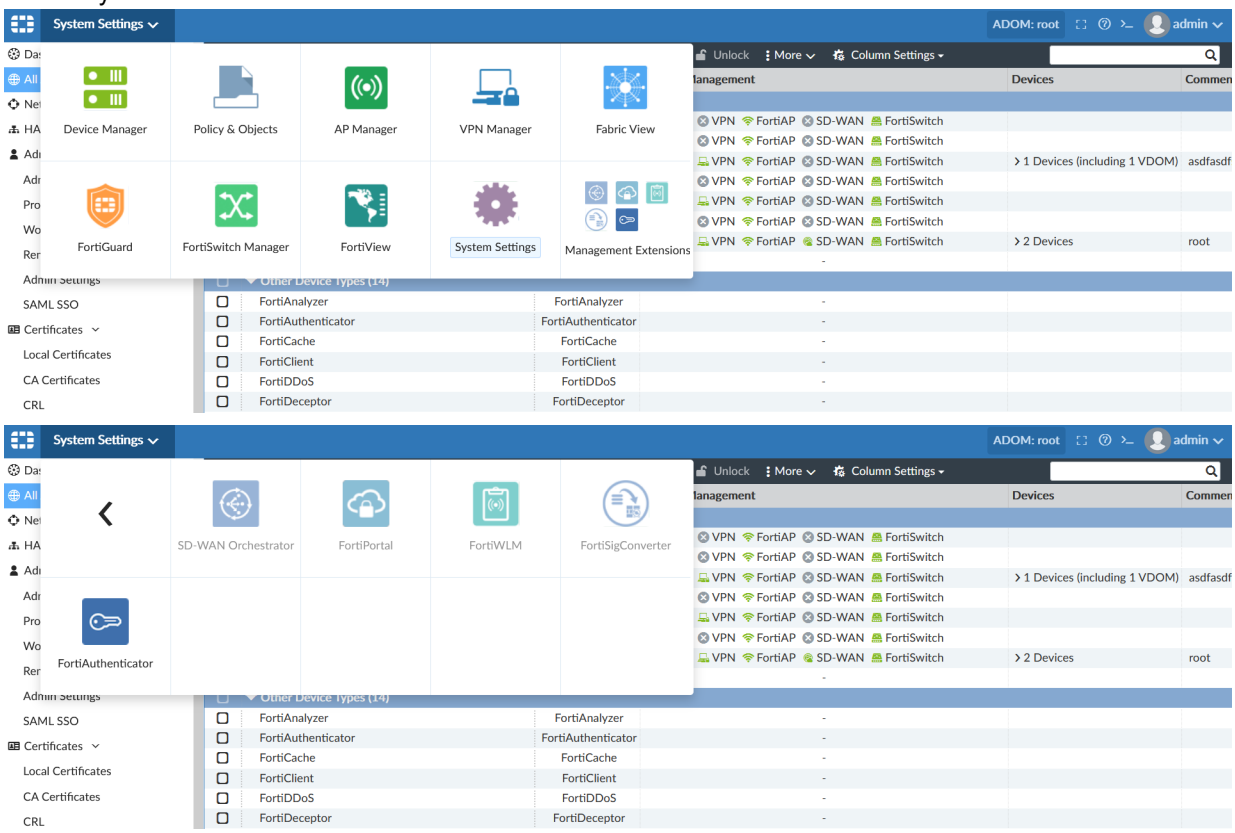
New management extension - FortiAuthenticator added to FortiManager - 6.4.3

The FortiAuthenticator management extension application has been added to FortiManager.

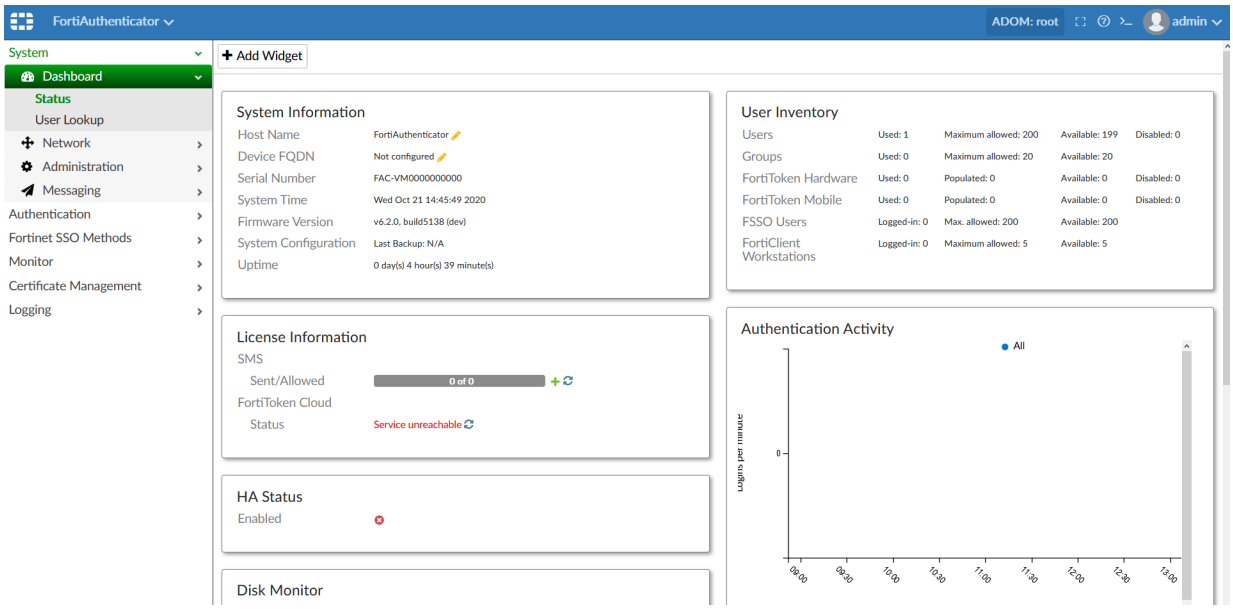
To use the FortiAuthenticator management extension application:

1. By default, the FortiAuthenticator management extension is disabled. You can enable it through the CLI or by clicking on the grayed-out *FortiAuthenticator* tile in *Management Extensions* when the *Management Extensions* tile

is already enabled.

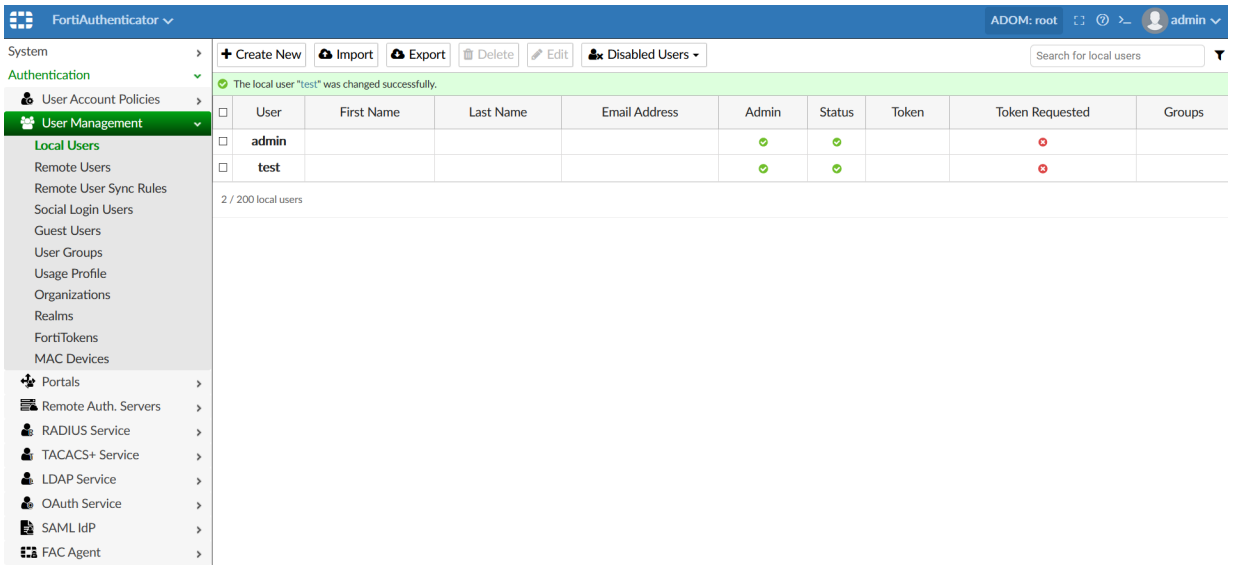


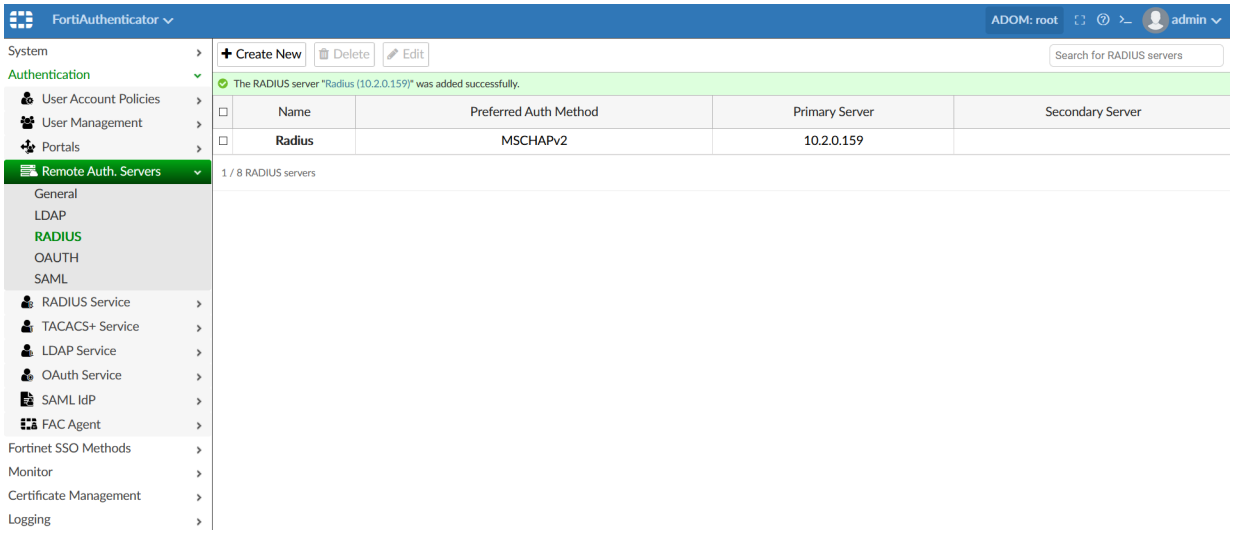
2. Once enabled, go to *Management Extensions* > *FortiAuthenticator* to view the FortiAuthenticator management extensions GUI.

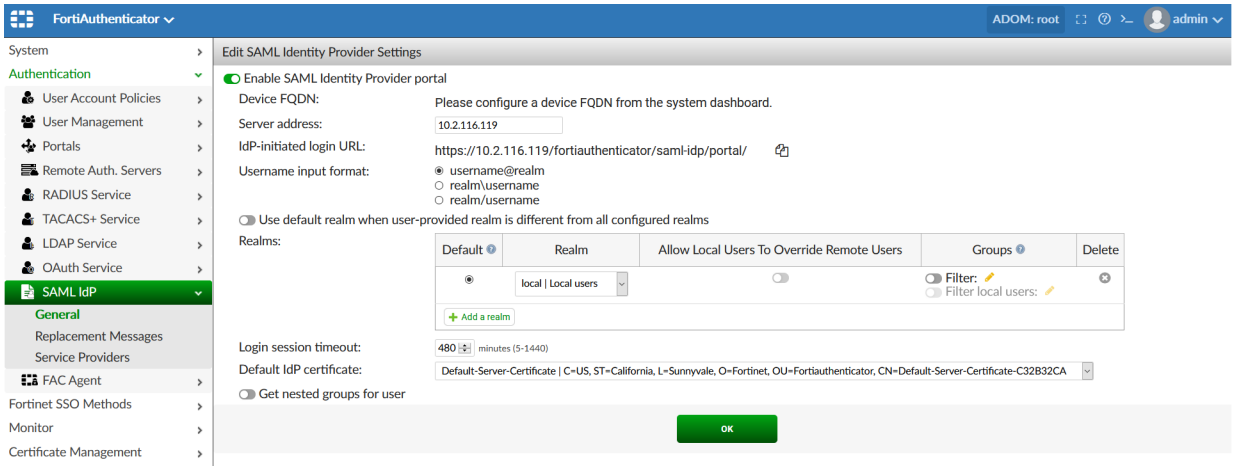


The FortiAuthenticator management extension includes the same capabilities as the standalone FortiAuthenticator product. See the FortiAuthenticator MEA Release Notes for exceptions.

You can use the FortiAuthenticator management extension to configure authentication requirements. For example, create local or remote users, create LDAP and RADIUS servers, and configure SAML authentication.


FortiAuthenticator
ADOM: root
admin
System
Authentication
User Account Policies
User Management
Local Users
Remote Users
Remote User Sync Rules
Social Login Users
Guest Users
User Groups
Usage Profile
Organizations
Realms
FortiTokens
MAC Devices
Portals
Remote Auth. Servers
RADIUS Service
TACACS+ Service
LDAP Service
OAuth Service
SAML IdP
FAC Agent
Create New
Import
Export
Delete
Edit
Disabled Users
Search for local users
The local user "test" was changed successfully.
User
First Name
Last Name
Email Address
Admin
Status
Token
Token Requested
Groups
admin
test
2 / 200 local users


FortiAuthenticator
ADOM: root
admin
System
Authentication
User Account Policies
User Management
Portals
Remote Auth. Servers
General
LDAP
RADIUS
OAUTH
SAML
RADIUS Service
TACACS+ Service
LDAP Service
OAuth Service
SAML IdP
FAC Agent
Fortinet SSO Methods
Monitor
Certificate Management
Logging
Create New
Delete
Edit
Search for RADIUS servers
The RADIUS server "Radius (10.2.0.159)" was added successfully.
Name
Preferred Auth Method
Primary Server
Secondary Server
Radius
MSCHAPv2
10.2.0.159
1 / 8 RADIUS servers


FortiAuthenticator
ADOM: root
admin
System
Authentication
User Account Policies
User Management
Portals
Remote Auth. Servers
RADIUS Service
TACACS+ Service
LDAP Service
OAuth Service
SAML IdP
General
Replacement Messages
Service Providers
FAC Agent
Fortinet SSO Methods
Monitor
Certificate Management
Edit SAML Identity Provider Settings
Enable SAML Identity Provider portal
Device FQDN:
Please configure a device FQDN from the system dashboard.
Server address:
10.2.116.119
IdP-initiated login URL:
https://10.2.116.119/fortiauthenticator/saml-idp/portal/
Username input format:
username@realm
realm\username
realm/username
Use default realm when user-provided realm is different from all configured realms
Realms:
Default
Realm
Allow Local Users To Override Remote Users
Groups
Delete
local | Local users
Filter:
Filter local users:
Add a realm
Login session timeout:
480
minutes (5-1440)
Default IdP certificate:
Default-Server-Certificate | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Fortiauthenticator, CN=Default-Server-Certificate-C32B32CA
Get nested groups for user
OK

To enable the FortiAuthenticator management extension through the CLI:

1. In the FortiManager CLI, enter the following commands.

```
config system docker
   set status enable
   set fortiauthenticator enable
end
```

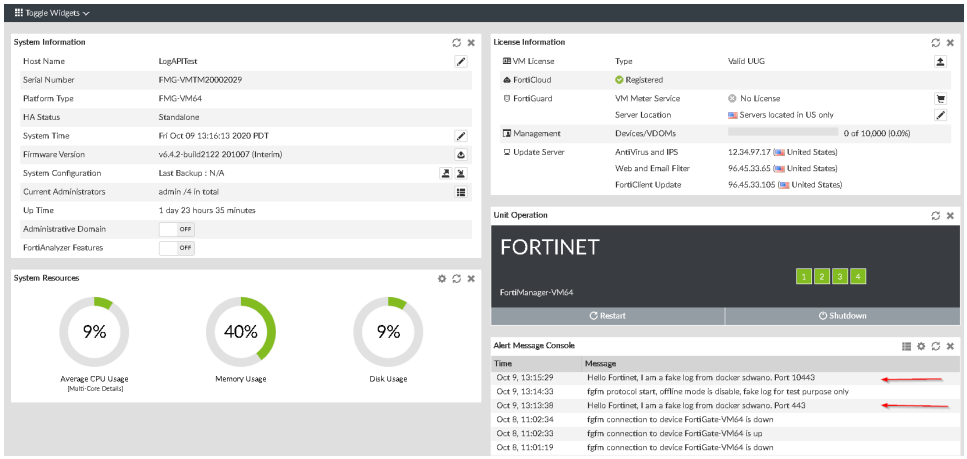
Management extension logs can be accessed in FortiManager or forwarded to FortiAnalyzer to analyze them further - 6.4.3

Event logs generated by a management extension are available in the local event log of FortiManager. They are displayed in the following locations in *System Settings*:

- *Alert Message Console* widget
- *Event log* pane

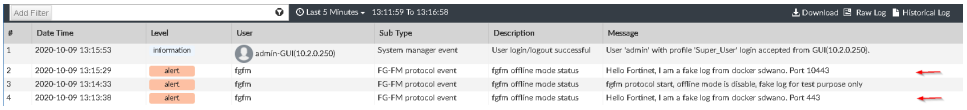
To access management extension logs in the *Alert Message Console* widget:

1. Go to *System Settings* > *Dashboard*.
2. In the *Dashboard* pane, locate the *Alert Message Console* widget.
   The recently generated management extension local logs are displayed in the *Alert Message Console* widget.



To access management extension logs in the *Event log* pane:

1. Go to *System Settings* > *Event Log* to view the local log list.
   The recently generated management extension local logs are displayed in the *Event Log* pane.

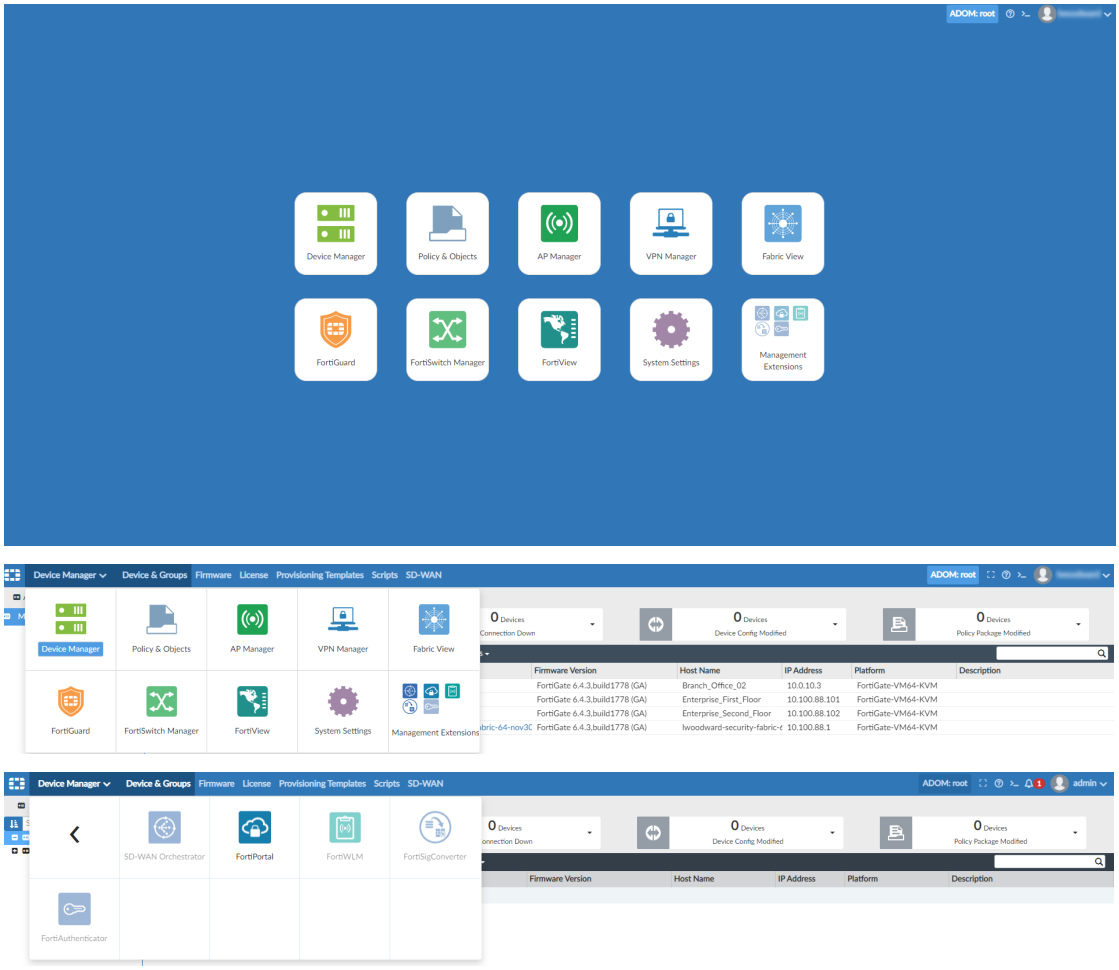


New management extension - FortiPortal added to FortiManager - 6.4.4

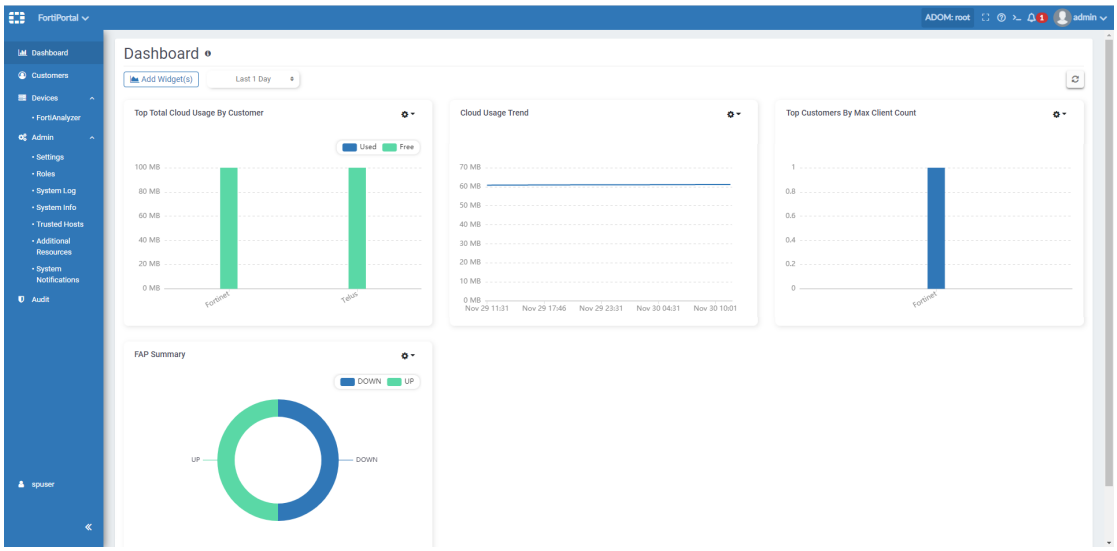
FortiPortal management extension application has been added as an integrated solution to FortiManager.

To use the FortiPortal management extension application:

1. By default, the FortiPortal management extension is disabled. You can enable it through the CLI or by clicking on the grayed out *FortiPortal* tile in *Management Extensions* when the *Management Extensions* tile is already enabled.

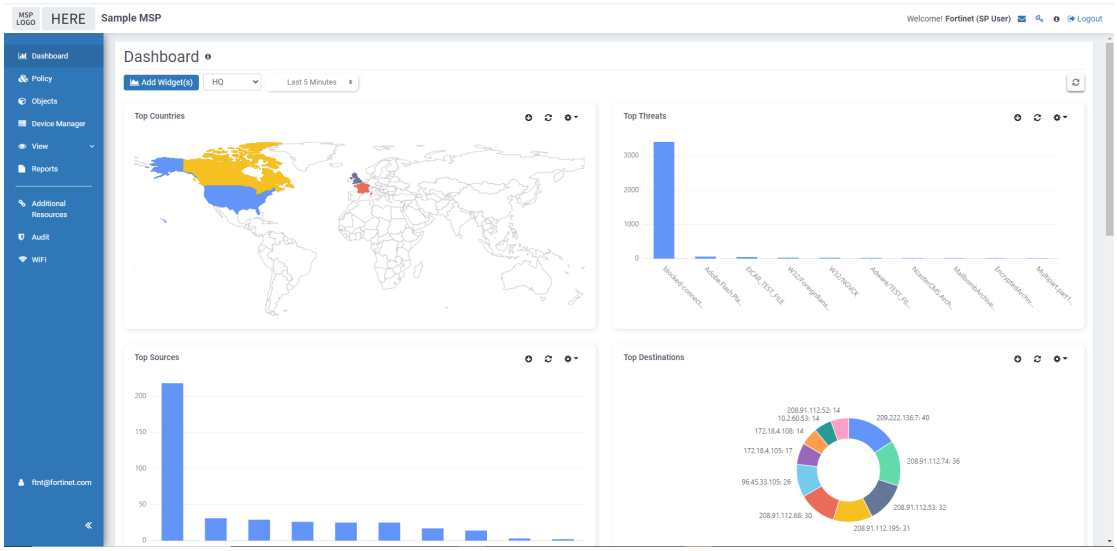


Once the FortiPortal management extension is successfully downloaded and launched, the user is automatically logged in as a super user (Super_User).



The function of adding a FortiManager is removed. You can only add FortiAnalyzer devices to the FortiPortal management extension.

The customer portal is same as the one in the standalone FortiPortal.

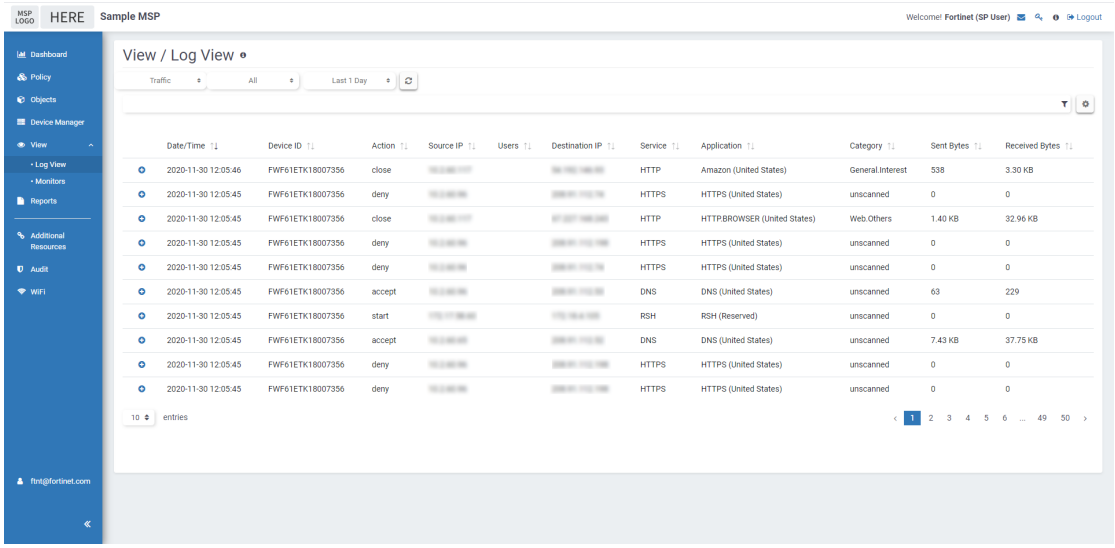


The header customization on the customer portal is not available yet.

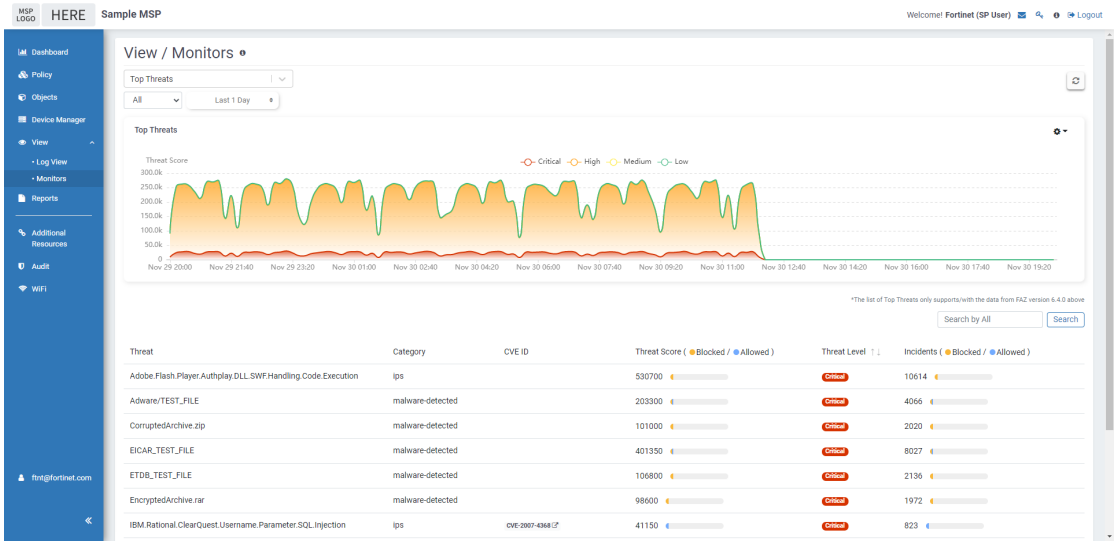
The FortiPortal management extension includes similar capabilities as the standalone FortiPortal. See the FortiPortal MEA Release Notes for exceptions.

You can use the *Log View* and the *Monitors* tab in *View* on the customer portal to display event logs and monitoring information for a customer.

The figure below shows an example of the *Traffic* tab in *View* > *Log View* that displays event logs grouped by application.



The figure below shows an example of the *Top Threats* tab in *View* > *Monitors* that displays threat information.



To enable the FortiPortal management extension through the CLI:

1. In the FortiManager CLI, enter the following commands:

```
config system docker
   set status enable
   set fortiportal enable
end
```

Licensing

FortiPortal MEA includes a free license. With the free license, you can manage 3 FortiGates or 3 VDOMs that are managed by FortiManager. If you want to manage additional devices or VDOMs with FortiPortal MEA, the following license is required:

- FortiPortal Subscription license for FPC VM-S.

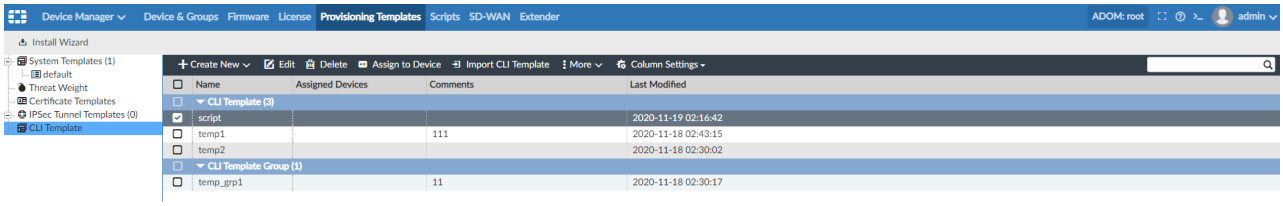
CLI Templates and Scripts usability improvements - 6.4.4

A few tabs of the *Device Manager* like *Device & Groups*, *Provisioning Templates*, and *Scripts* have been improved for a better user experience.

The *CLI Template* and *CLI Template Group* entries can now be accessed from the *Provisioning Templates* tab instead of the *Scripts* tab.

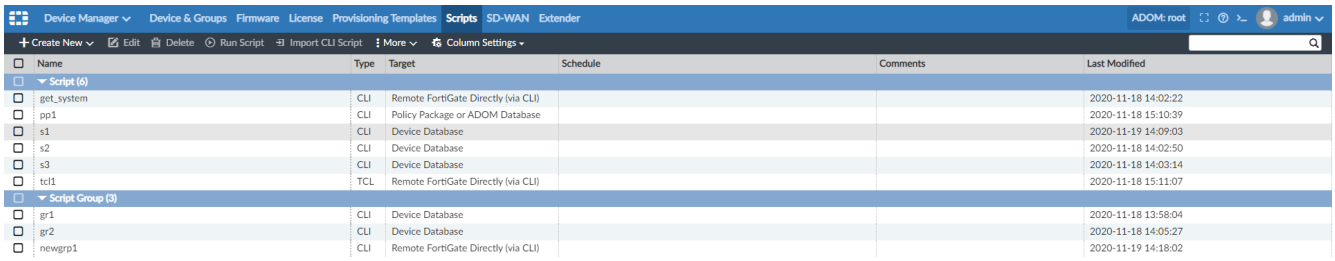
To view the *CLI Template* and *CLI Template Group* entries:

1. Go to *Device Manager* > *Provisioning Templates*.
2. Click *CLI Templates* from the tree menu.



The *Script* and *Script Group* entries are consolidated and appear together in the content pane of the *Scripts* tab, and the tree menu is removed from the *Scripts* tab for a wider content pane.

Go to *Device Manager* > *Scripts* to view the *Script* and *Script Group* entries.

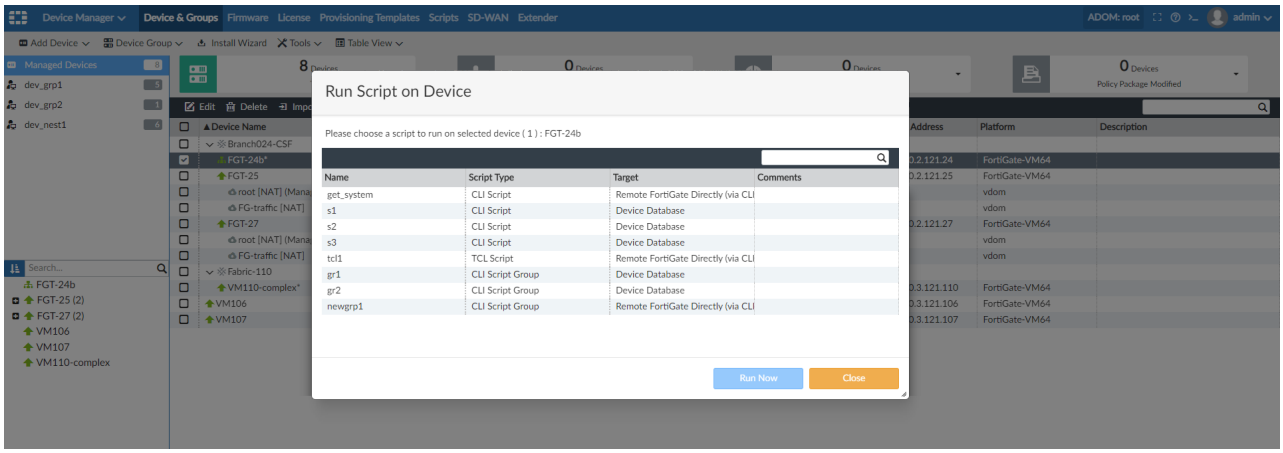


When attempting to run scripts on a managed device, the *Run Script on Device* dialog displays *Script Group* entries in addition to *Script* entries.

To run *Script* and/or *Script Group* entries on managed devices:

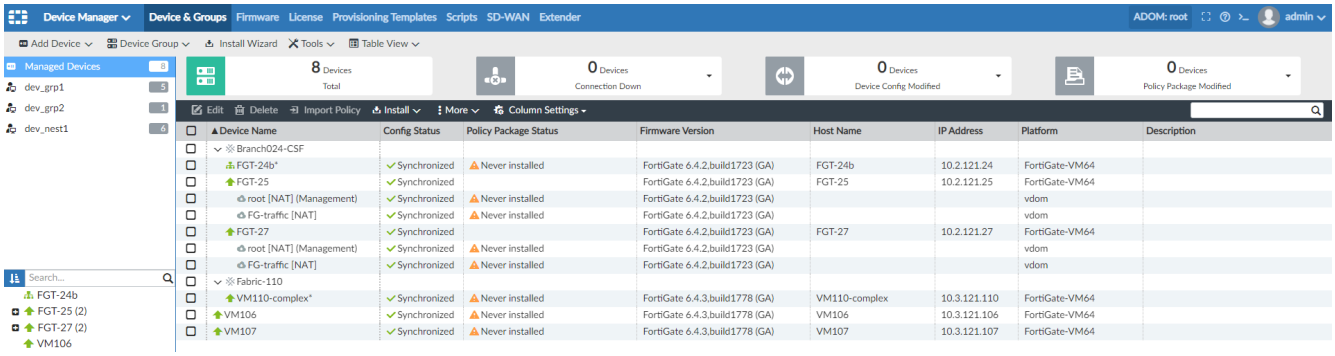
1. Go to *Device Manager* > *Device & Groups*.
2. Click *Managed Devices* from the tree menu, and select a device from the table.
3. Either right-click the selected device or click on *More* from the toolbar above, and click *Run Script*. The *Run Script on Device* dialog appears.
4. Select either a *Script* entry or a *Script Group* entry from the table.

5. Click *Run Now* to run the selected entry on the managed device.



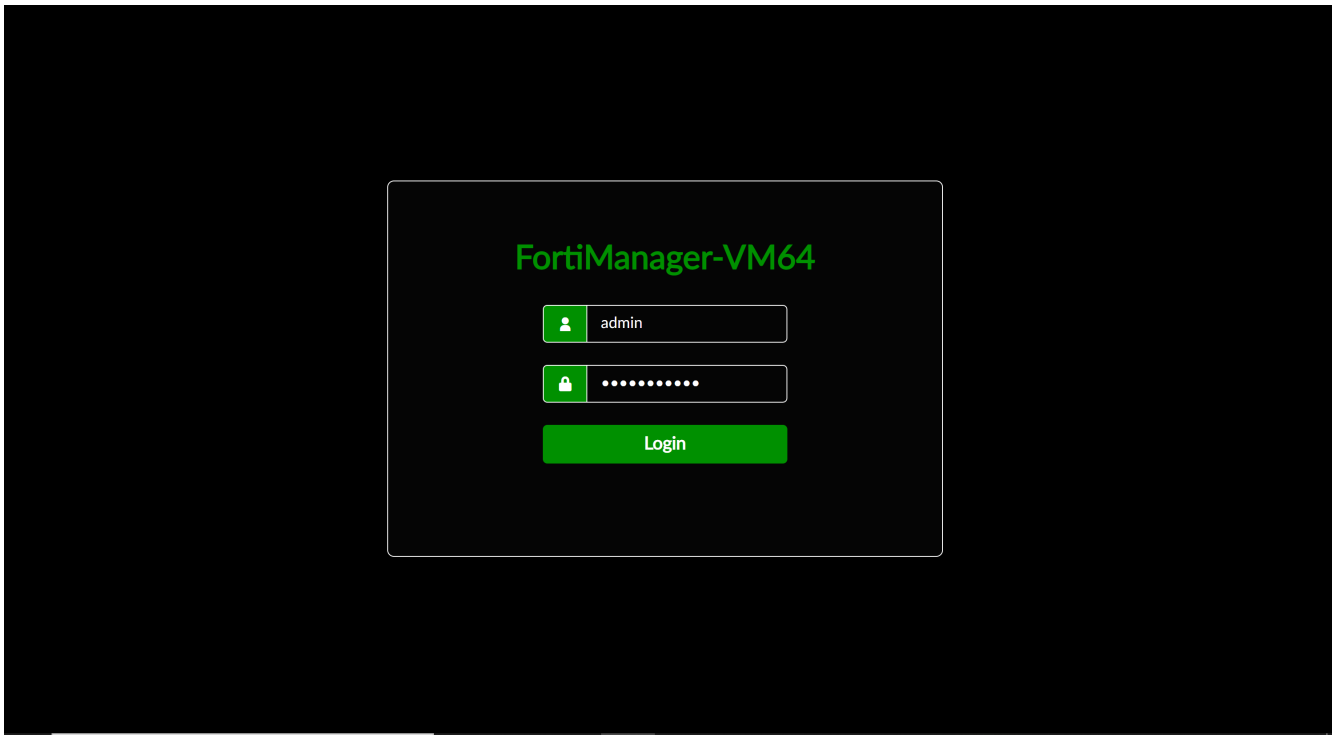
When viewing a *Security Fabric* group entry from the *Managed Devices* table, the fabric group entry does not display in a collapsed view by default. The group entry is displayed in an expanded view and the device listings within the group entry are displayed by default.

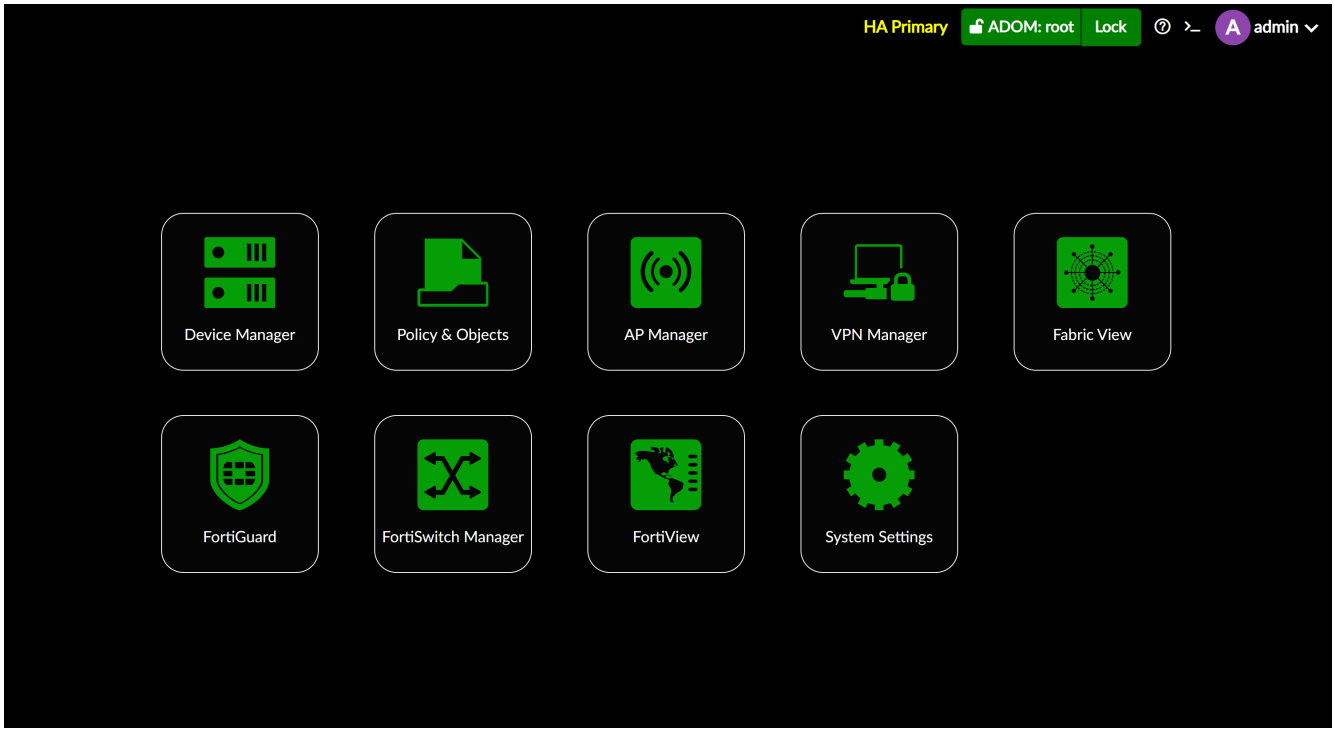
Go to *Device Manager* > *Device & Groups*, and click *Managed Devices* from the tree menu to view the managed devices and group entries in an expanded view by default.

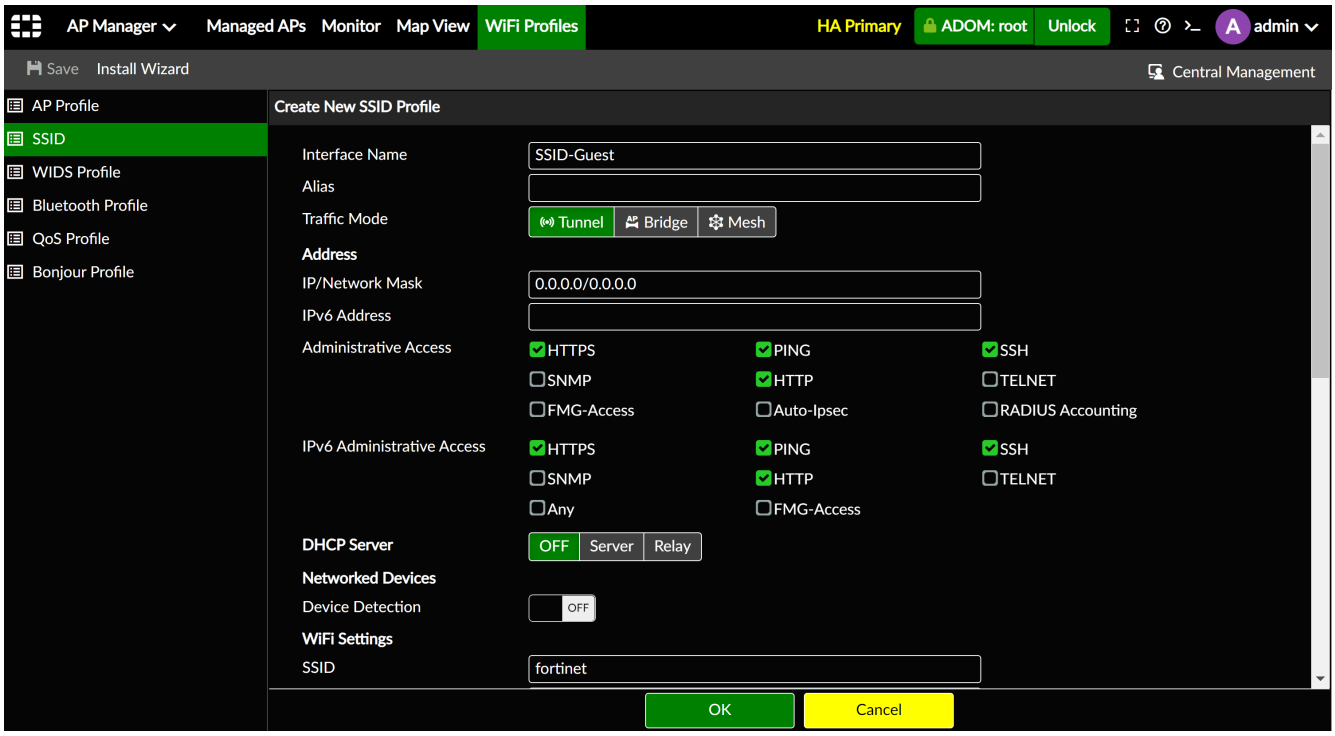


FortiManager GUI accessibility improvements - 6.4.4

FortiManager now implements a high contrast dark theme in order to make the FortiManager GUI more accessible, and to aid people with visual disability in using the FortiManager GUI.


FortiManager-VM64
admin
Login


HA Primary
ADOM: root
Lock
admin
Device Manager
Policy & Objects
AP Manager
VPN Manager
Fabric View
FortiGuard
FortiSwitch Manager
FortiView
System Settings



To change the currently active theme to the *High Contrast Dark* theme:

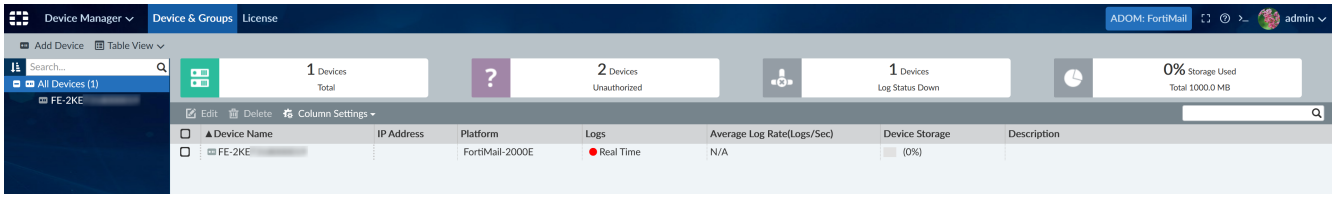
1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. Scroll to *View Settings* > *Theme*.
3. Select the *High Contrast Dark* theme tile from the available theme tiles.

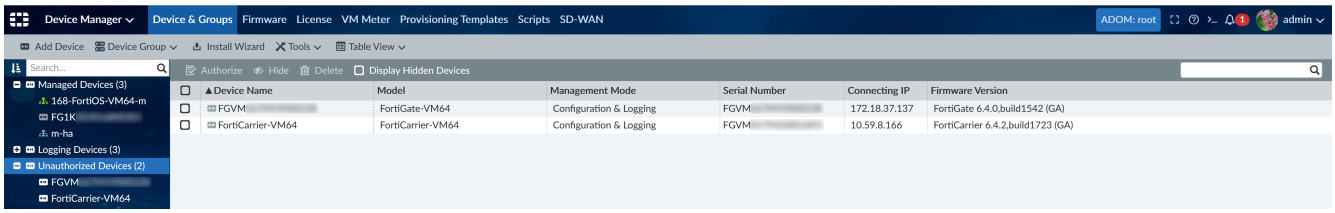
4. Click *Apply*.

Device authorization usability improvements - 6.4.4

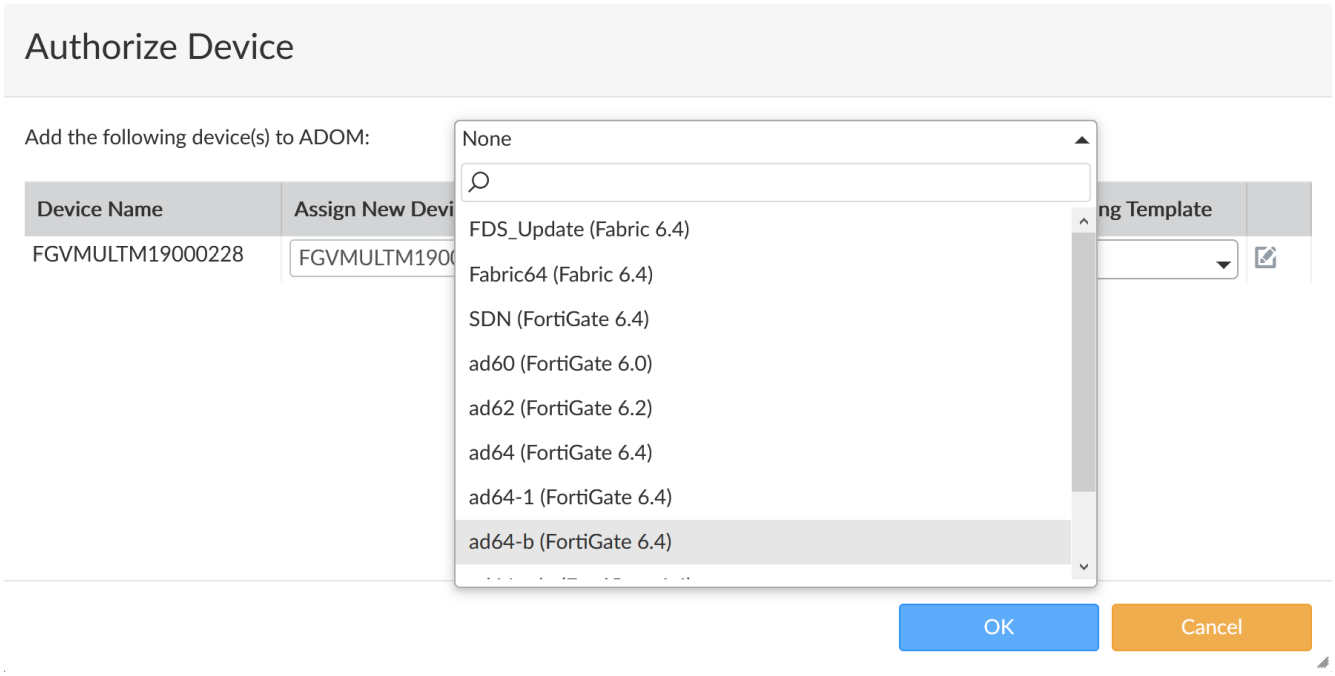
This version of FortiManager improves device authorization usability for a better user experience.

From a non-root ADOM under *Device Manager* > *Device & Groups*, clicking on the *X Devices Unauthorized* tile in the quick status bar does not simply refresh the device list but redirects to the *Unauthorized Devices* page and displays the unauthorized devices in the content pane of the root ADOM.

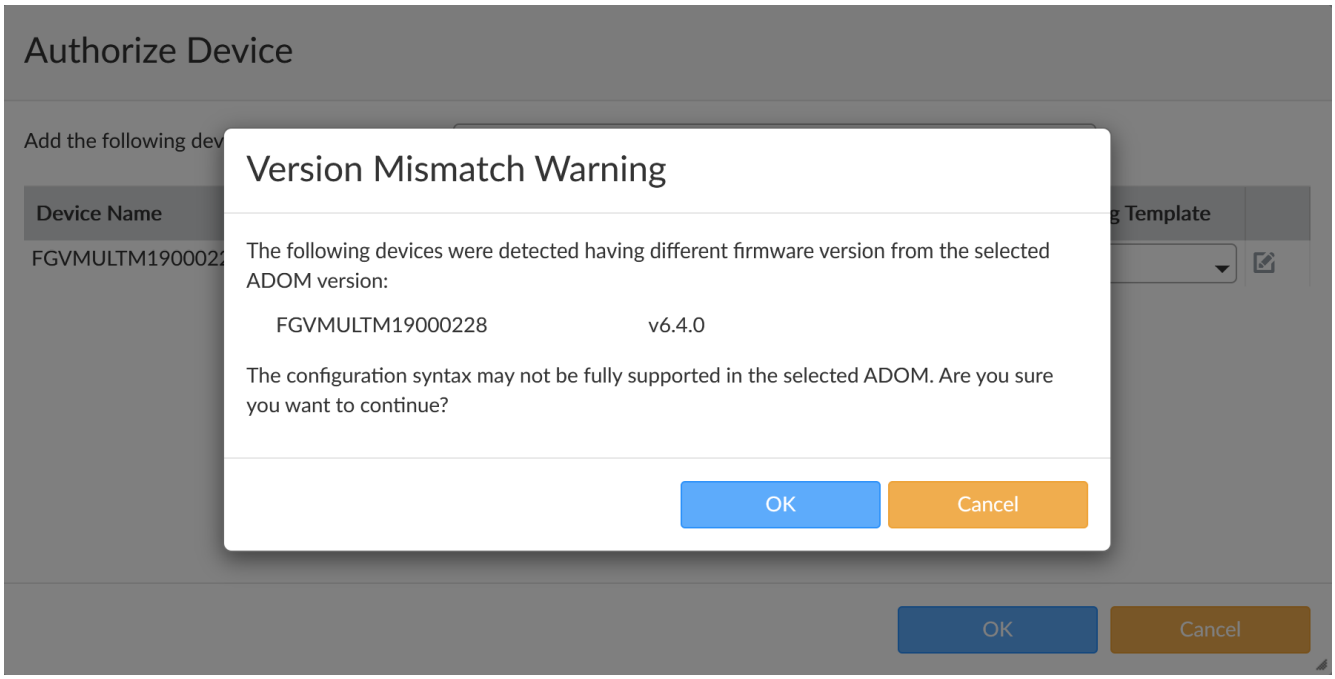




When authorizing devices from the root ADOM, the *Authorize Device* dialog has `None` selected by default instead of `root` in the ADOM selection drop-down list.



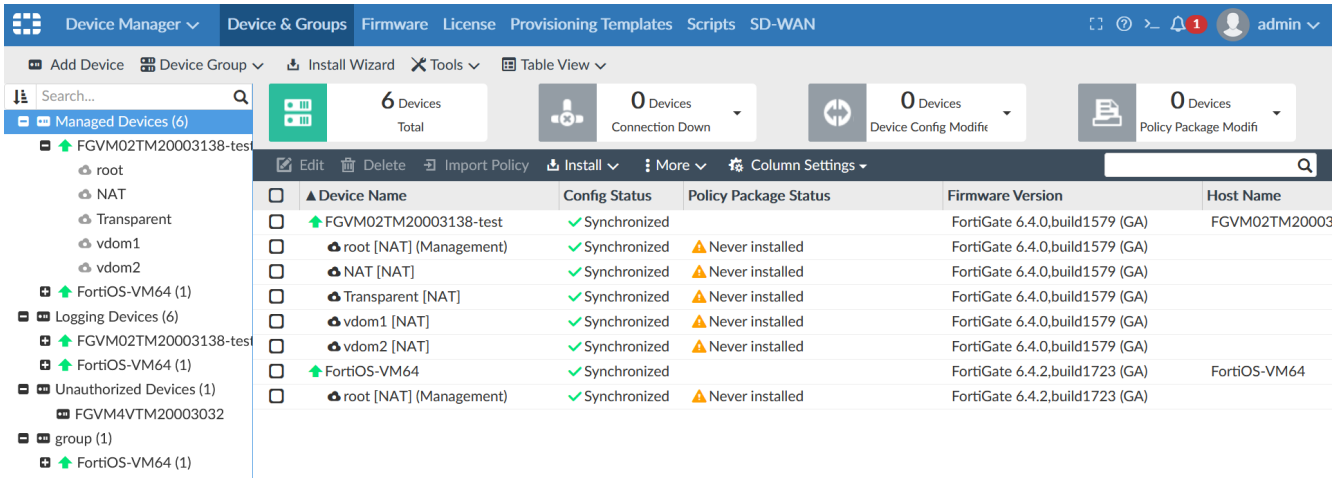
If the devices selected to be authorized have a different firmware version than the ADOM versions the devices are added to, the FortiManager system displays a *Version Mismatch Warning* confirmation dialog before proceeding with the authorization.



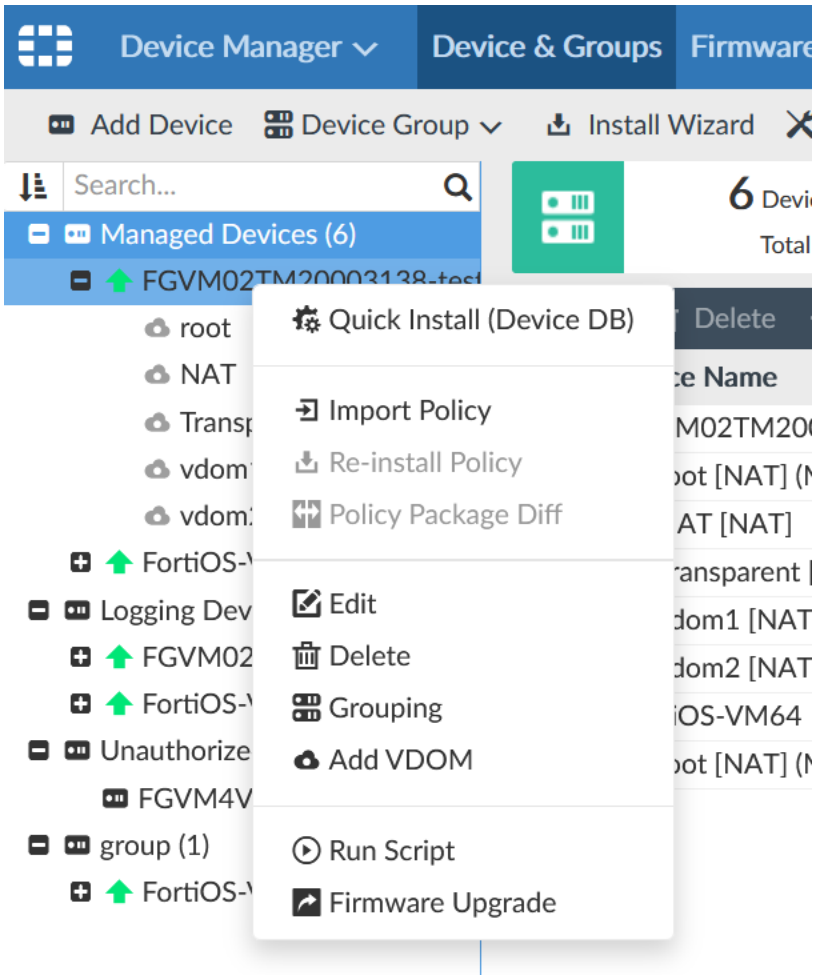
Device manager usability improvements - 6.4.4

This version of FortiManager improves device manager usability for a better user experience.

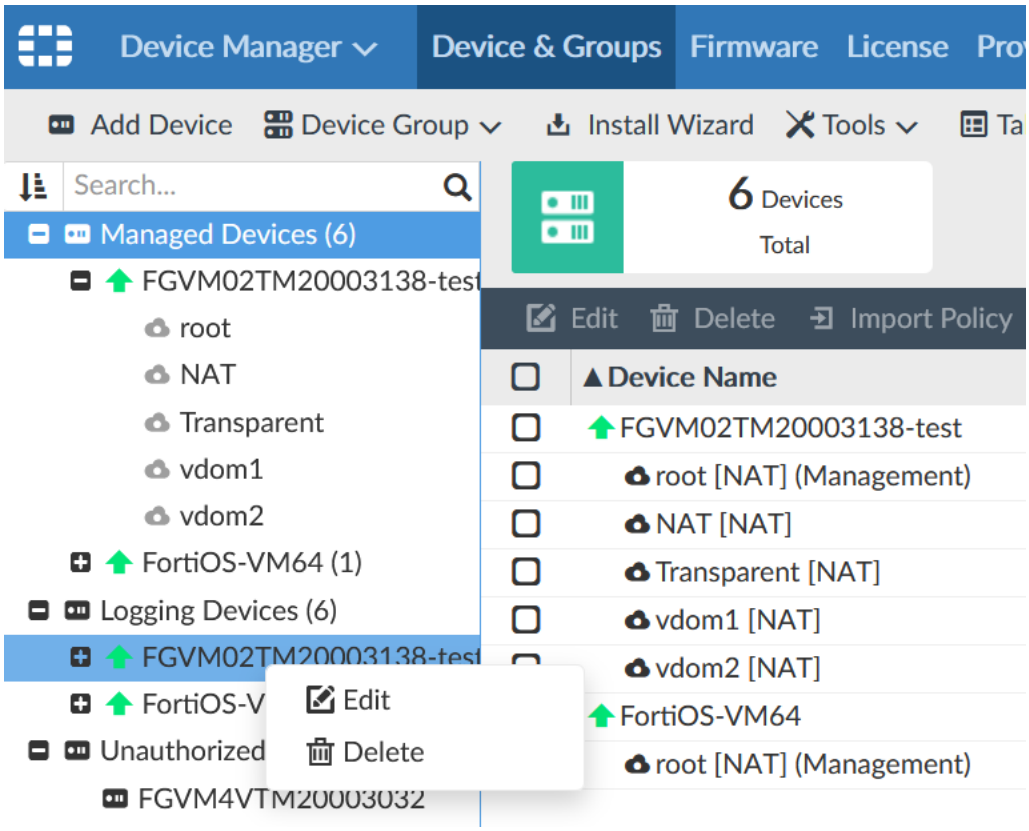
Devices are categorized and listed in a hierarchical tree menu into various categories like *Managed Devices* for all the managed devices, *Logging Devices* if FortiAnalyzer features are enabled, *Unauthorized Devices* for devices that are not authorized, and custom groups if created.



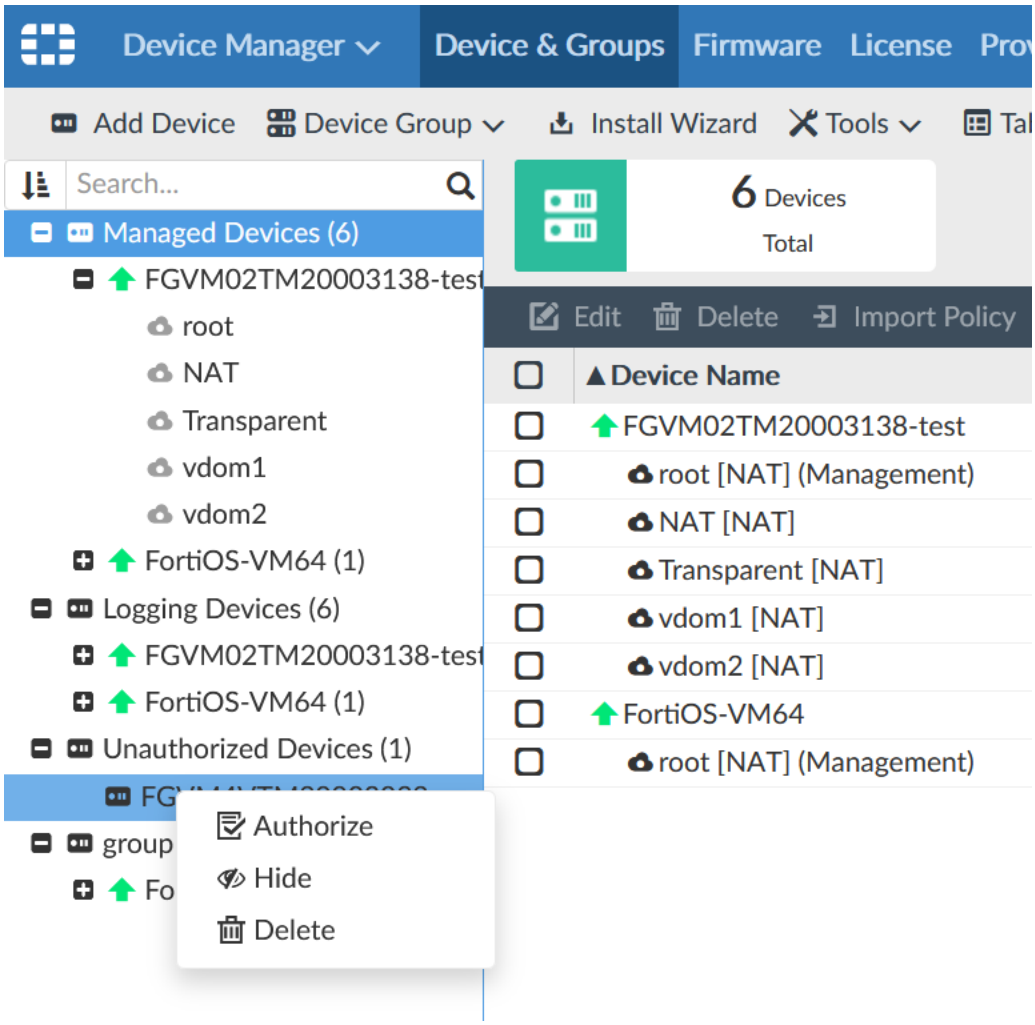
The right-click menu lists more options like *Quick Install*, *Import Policy*, *Edit*, *Delete*, and so on, to facilitate the user to take actions from the tree menu.



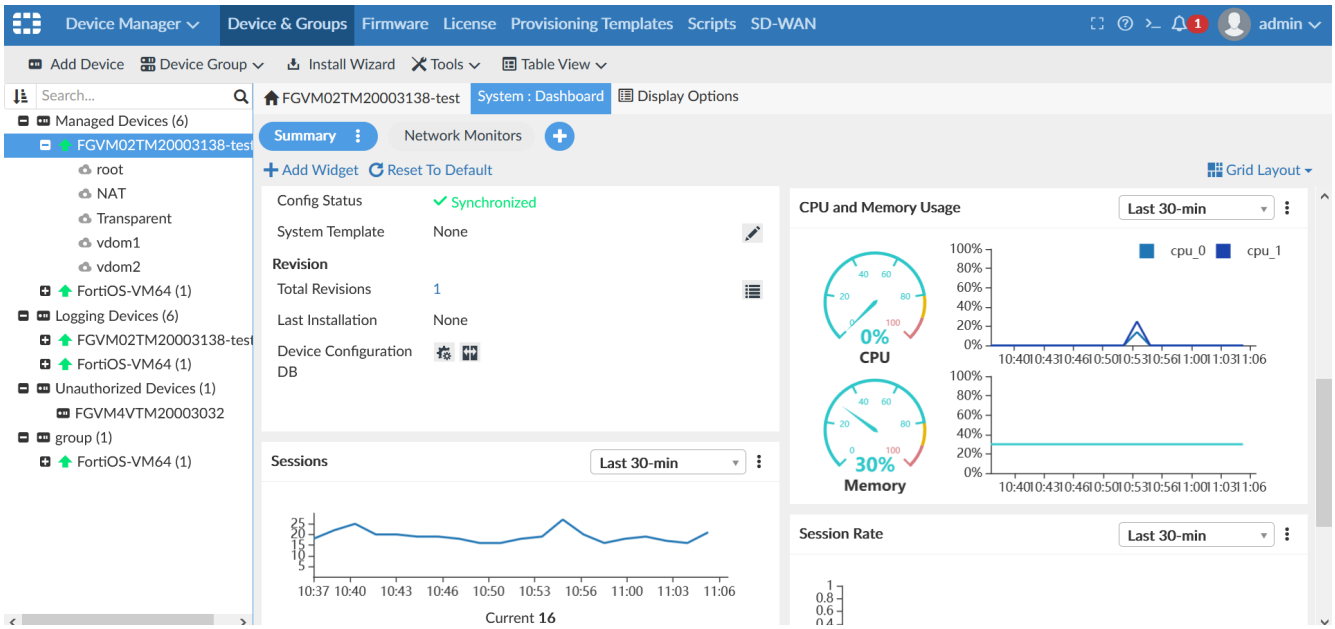
You may *Edit* or *Delete* a device listed under the *Logging Devices* category in the tree menu.



You may *Authorize*, *Hide*, or *Delete* a device listed under the *Unauthorized Devices* category in the tree menu.



The *System: Dashboard* tab now lists widgets under *Summary* and *Network Monitors*.



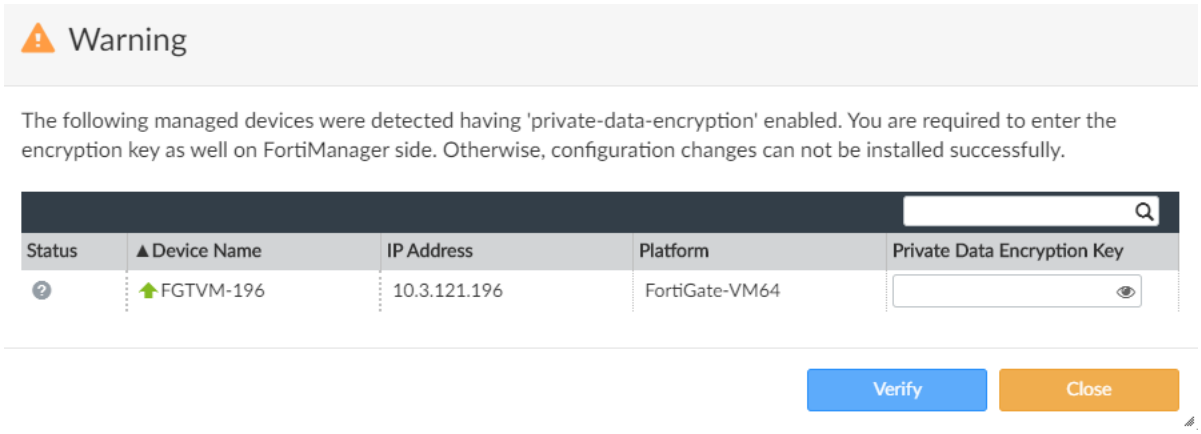
FortiOS private data encryption support - 6.4.4

FortiManager supports the private data encryption settings on FortiOS. FortiGates with the `private-data-encryption` setting enabled can be managed by FortiManager.

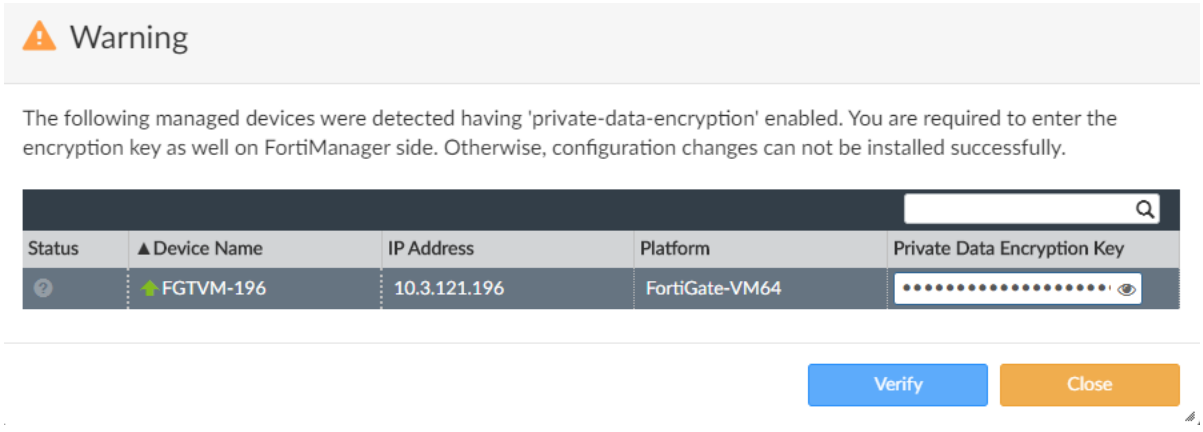
When a FortiGate with the `private-data-encryption` setting enabled is added to FortiManager, FortiManager requires the FortiGate encryption key to be entered in FortiManager to successfully install device configuration settings and manage the added FortiGate. To know more about adding devices to FortiManager, see the FortiManager Administration Guide on the Docs Library.

To verify an added FortiGate with its encryption key on FortiManager:

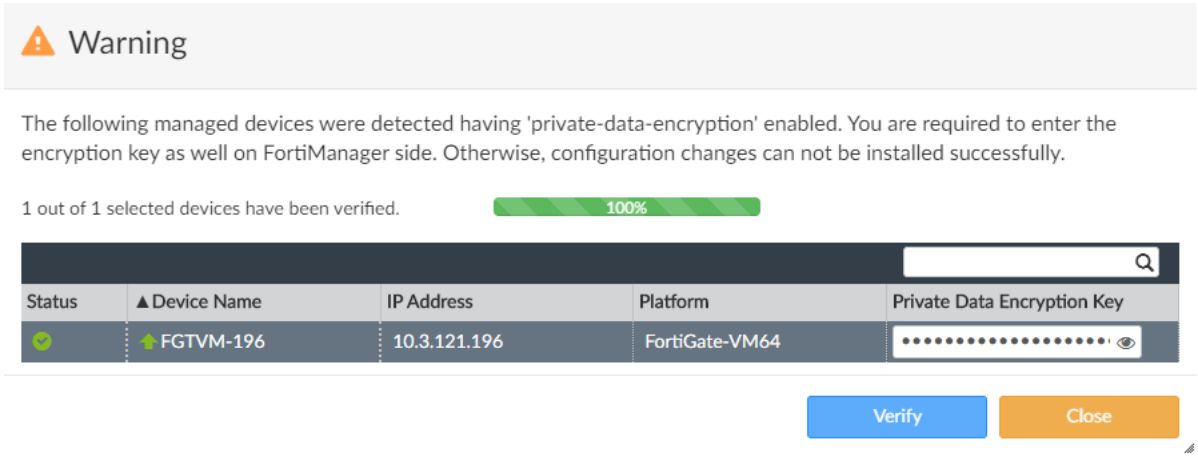
1. Go to *Device Manager*. The *Device Manager* prompts with a *Warning* dialog that requires the FortiGate encryption key to be entered:



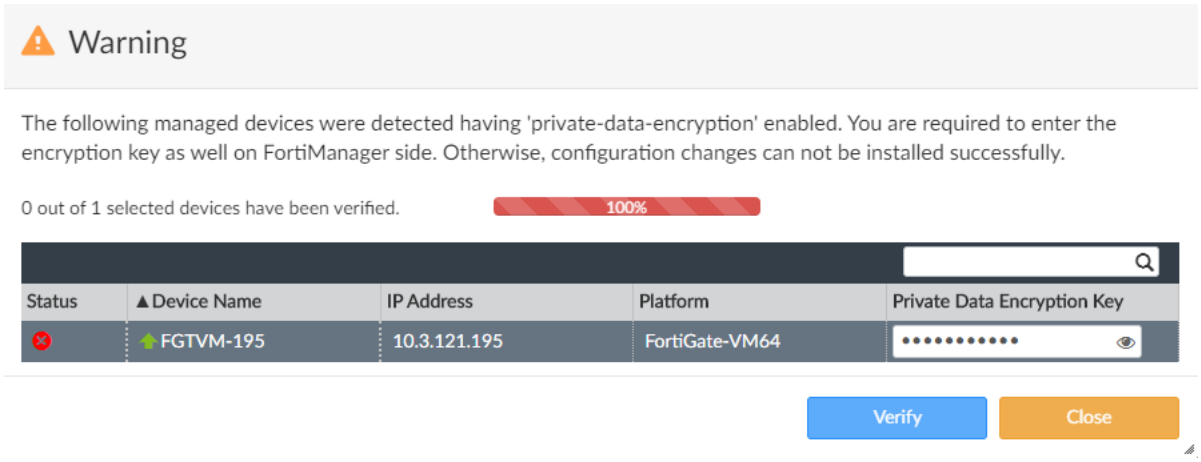
2. Enter the correct encryption key into the *Private Data Encryption Key* field for each of the listed FortiGates. The *Warning* dialog lists all the FortiGates for which the respective encryption keys are required.



3. Click *Verify*. If the encryption key matches, the device is verified.

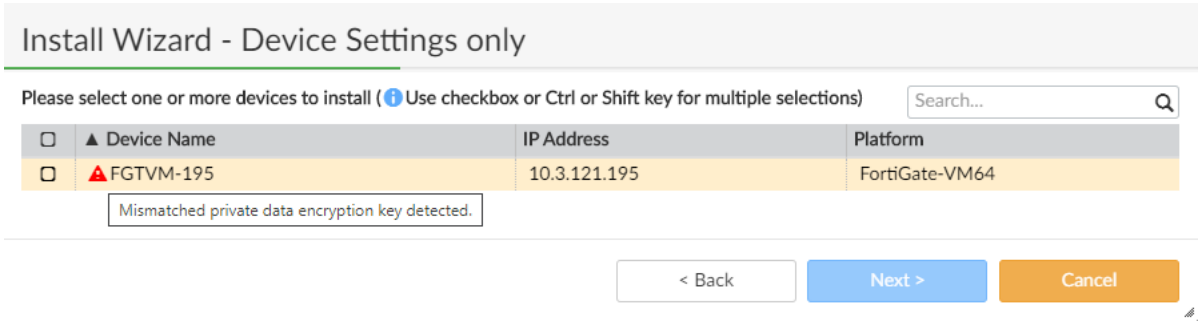


If the encryption key does not match, the verification fails, and you may try again with the correct key.



Once the added FortiGates are verified, you may start managing the added devices.

Every time you try to install configuration settings to the managed FortiGates, FortiManager checks if the FortiGate encryption is correct. If the encryption key is incorrect, the added device is disabled for installation.



You may verify devices again from the *Device Manager* by entering the correct encryption keys for the disabled FortiGates.

FortiManager does not support enabling or disabling the `private-data-encryption` setting on FortiOS. It must be done on the managed FortiGate. To learn more about it, see the FortiOS Administration Guide on the Docs Library.

If the `private-data-encryption` setting is enabled on an already managed FortiGate, you may need to manually retrieve device configuration settings again on FortiManager.

FortiSwitch Manager device monitoring usability improvements - 6.4.4

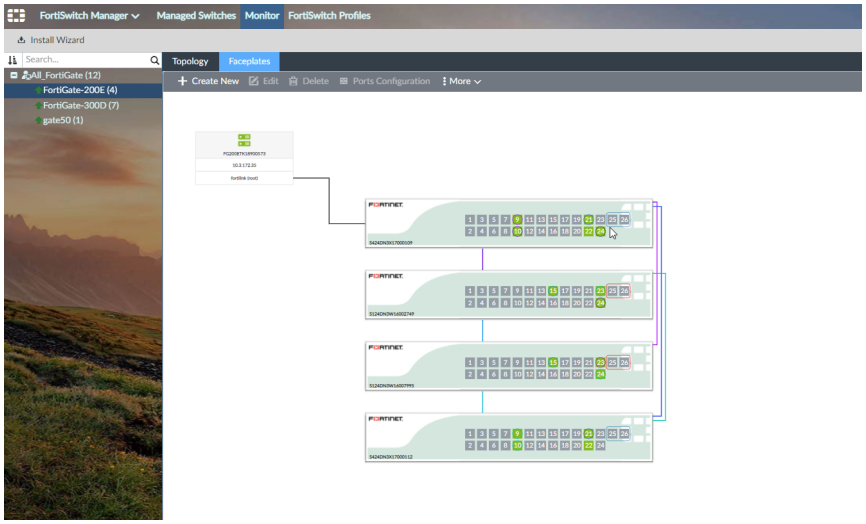
FortiSwitch Manager central mode device monitoring supports both the block-style topology representation and the faceplate or port status view.

You can change views to see both the faceplate and block-style topology diagram. This facilitates viewing the uplinks in the topology representation and which ports are up and down in the faceplate view. This is useful for troubleshooting and also to ascertain the state of ports before making any configuration changes.

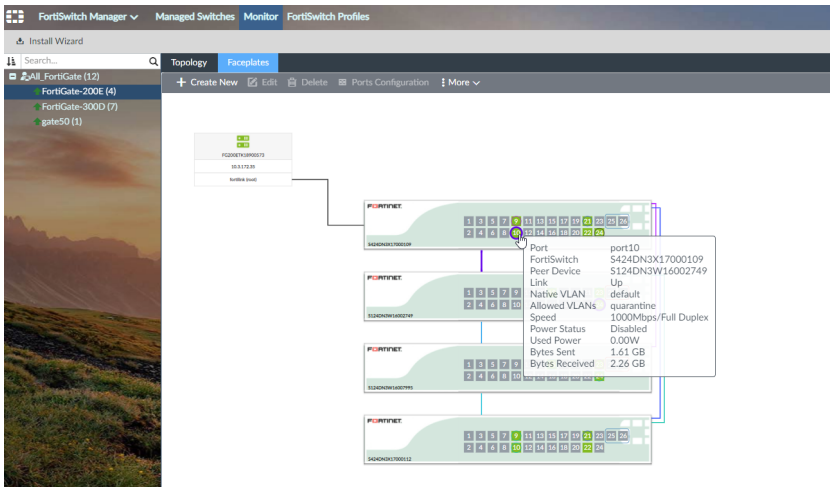
Go to *FortiSwitch Manager* > *Monitor* and click on *Topology* or *Faceplates* from the content pane to view the block-style topology diagram or the port status view respectively. Use the search box to find a specific device or filter the view, and hover over connections or ports to get more information.

To view faceplate topology:

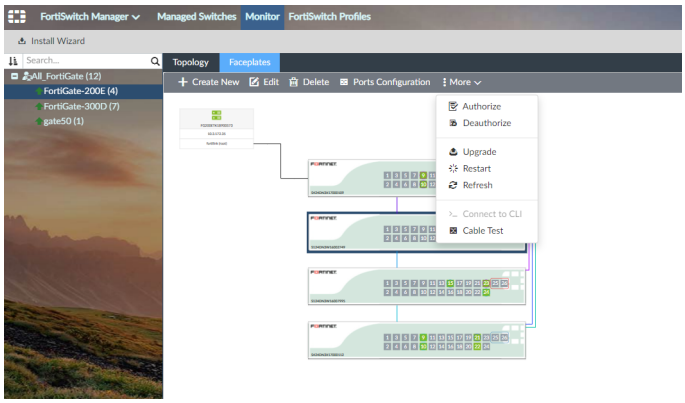
1. Go to *FortiSwitch Manager* > *Monitor* > *Faceplates*. The connection and ports statuses are displayed.



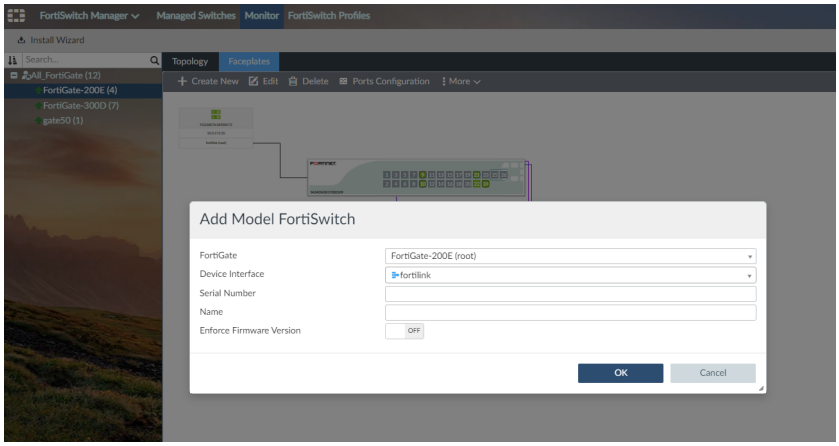
2. Hover over the switch port, to view detailed information about the port.



3. Select a switch in the tree-menu to edit the switch and view the port configuration. Right-click a port to authorize, deauthorize, or upgrade a device. You can also restart the switch or perform a cable test.



4. In the toolbar, click Create New to add a FortiSwitch.



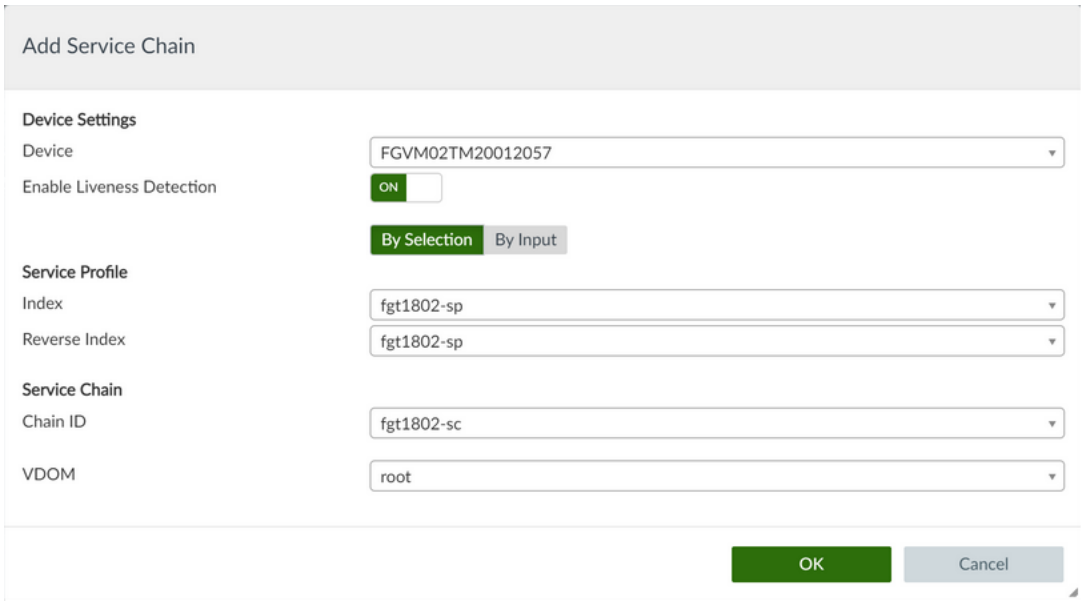
Liveness detection support for VMware NSX-T service - 6.4.4

The *Liveness Detection* feature may be used to force the VMware NSX-T service to not use a specific FortiGate device until its service managing FortiManager updates the FortiGate configuration. This is expected to be a common requirement when, for example, new FortiGates are deployed. If this is desired, the newly deployed FortiGates should not reply to liveness detection queries or forward any traffic until they have received sufficient configuration data from their service managing FortiManager. The VMware NSX-T service will use other already-configured FortiGates instead, if any are available.

When configuring a service from FortiManager to VMware NSX-T, you may set the *Enable Liveness Detection* setting to *ON* or *OFF*. The setting is *ON* by default.

To configure a VMware NSX-T service with *Liveness Detection*:

1. Register a service from FortiManager to VMware NSX-T. See *To register a service from FortiManager to VMware NSX-T* on the Creating VMware NSX-T connector page of the FortiManager 6.4.4 Admin Guide.
2. Deploy a FortiGate VM from VMware NSX-T and enable central management. See *To deploy a FortiGate VM from VMware NSX-T and enable central management* on the Creating VMware NSX-T connector page of the FortiManager 6.4.4 Admin Guide.
3. Add the service chain and configure the *Liveness Detection* setting:
   a. On the FortiManager GUI, go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *Endpoint/Identity* and select the added NSX-T service.
   b. Right-click on the selected service and click *Configure*. The *Configure Devices of NSX-T Service* dialog appears.
   c. Select the FortiGate device listed in the table and click *Add*. The *Add Service Chain* dialog appears.

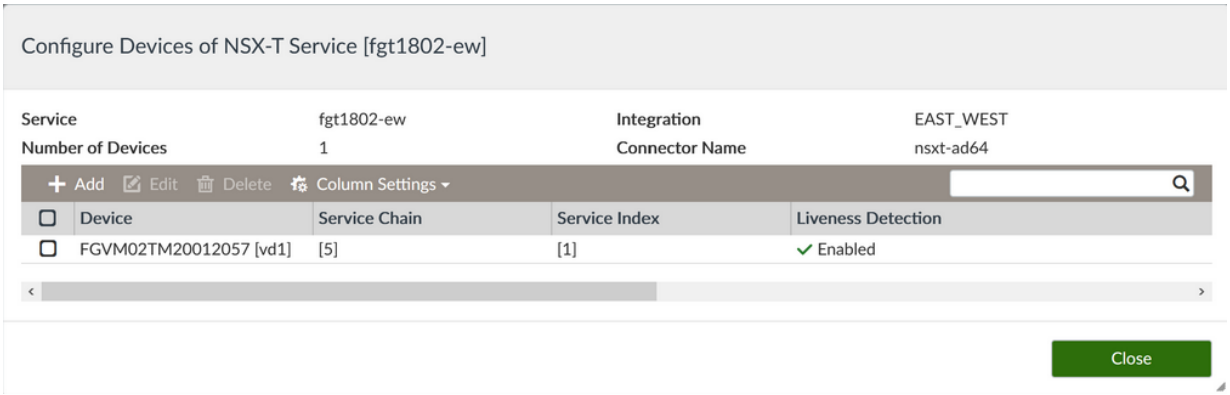


   d. Toggle the *Enable Liveness Detection* setting to *ON*. It is set to *ON* by default.
   e. Select the appropriate options for the *Service Profile* and *Service Chain* fields as required from the drop-down lists.
   f. Click *OK*.
4. Configure *Liveness Detection* and service chain configurations on FortiGate from the CLI:

```
FortiGate-VM64 # conf nsxt setting
FortiGate-VM64 (setting) # sh fu
```

```
config nsxt setting
   set liveness disable
   set service "<name>"
end
FortiGate-VM64 (setting) # set liveness enable
FortiGate-VM64 (setting) # end
FortiGate-VM64 #

FortiGate-VM64 (5) # sh
config nsxt service-chain
   edit 5
      config service-index
         edit 1
            set vd "root"
         next
      end
   next
end
FortiGate-VM64 (5) # end
```

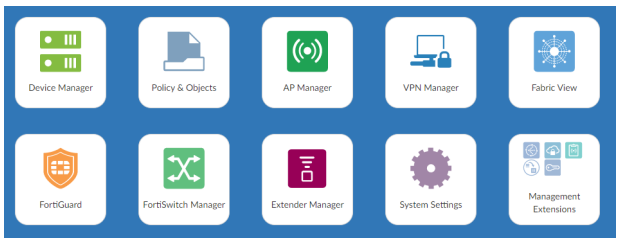
5. Check *Liveness Detection* and service chain configurations on FortiManager:
   a. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *Endpoint/Identity* and select the added NSX-T service.
   b. Right-click on the selected service and click *Configure*. The *Configure Devices of NSX-T Service* dialog appears. The *Liveness Detection* column indicates that the setting is *Enabled*.



6. Configure a virtual wire pair interface and a virtual wire pair policy and install to FortiGate. See *To complete the fabric connector setup* on the Creating VMware NSX-T connector page of the FortiManager 6.4.4 Admin Guide.

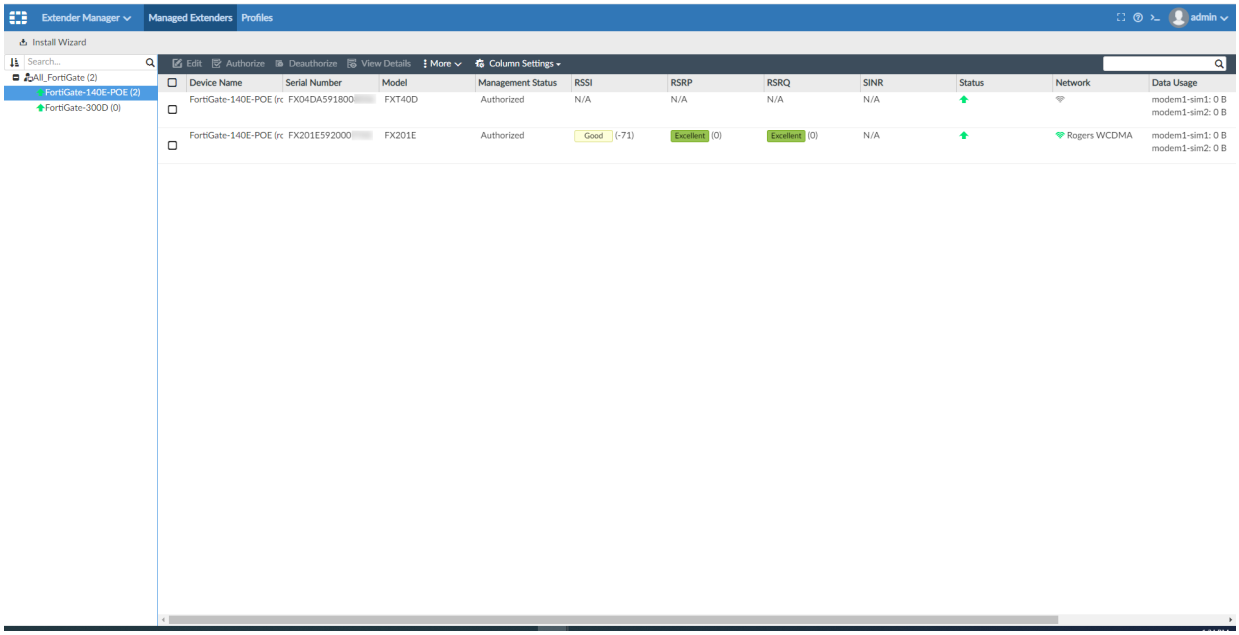
FortiExtender 6.4.2 dataplan and two modems support for FortiManager - 6.4.4

The new Extender Manager module appears when FortiManager detects a FortiGate that is connected to FortiExtender. You can use the module to configure two modems, as well as data plans and SIM profiles.

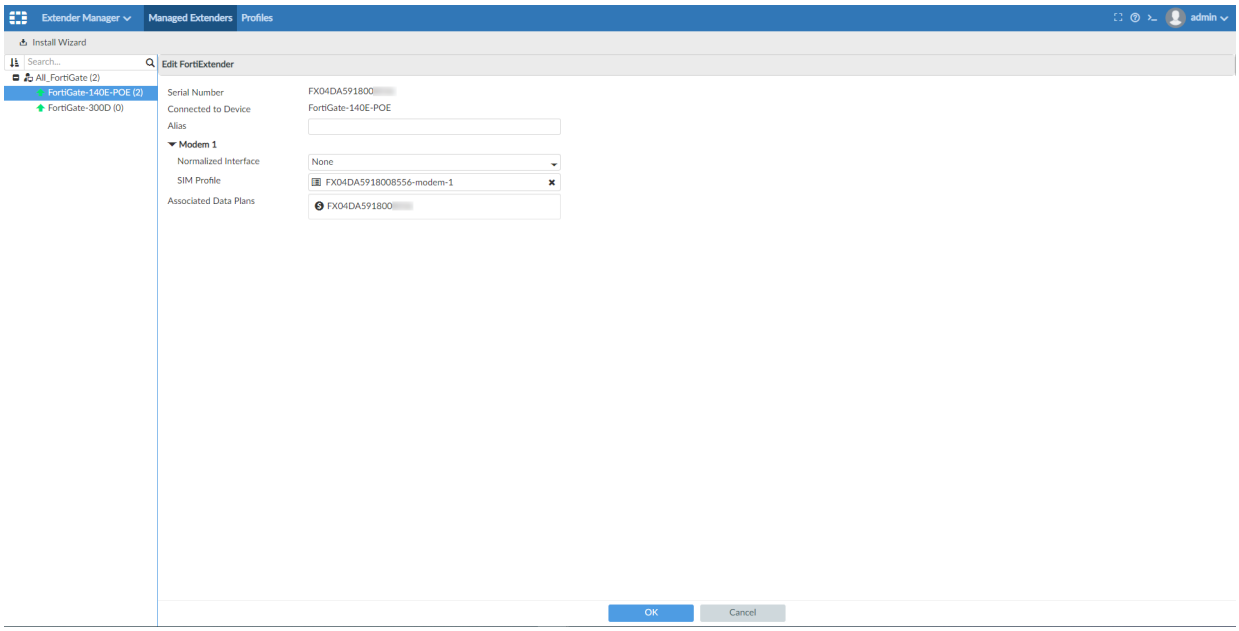


To view managed FortiExtenders:

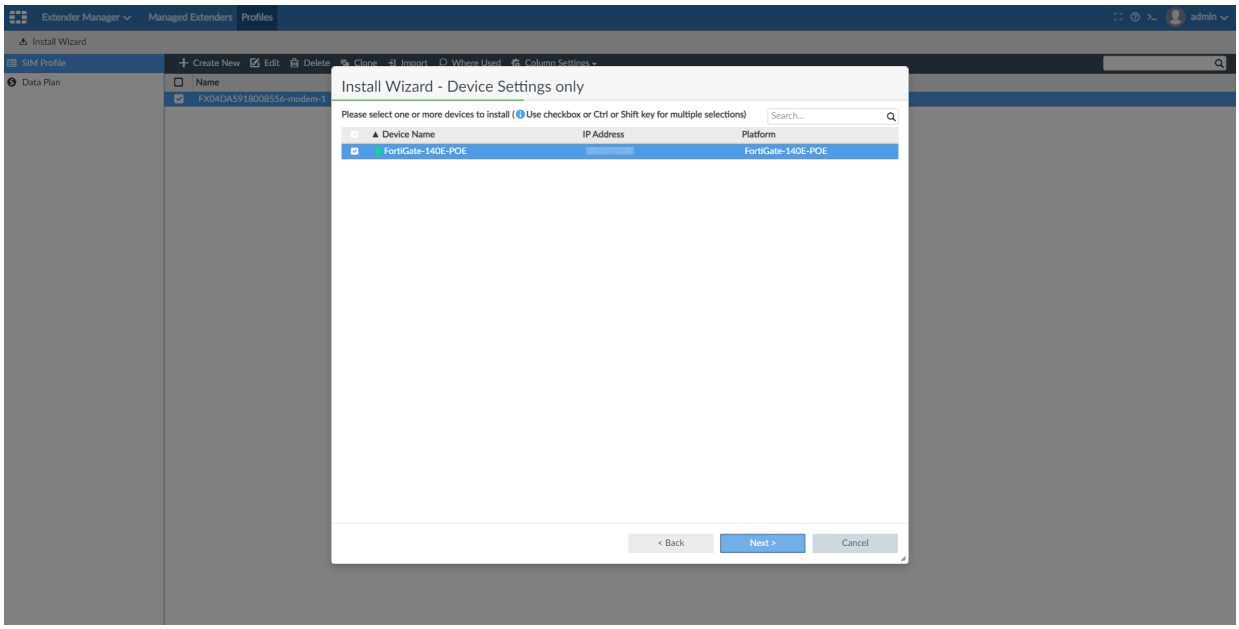
1. Go to*Extender Manager* > *Managed Extenders*. The managed FortiExtenders are displayed.



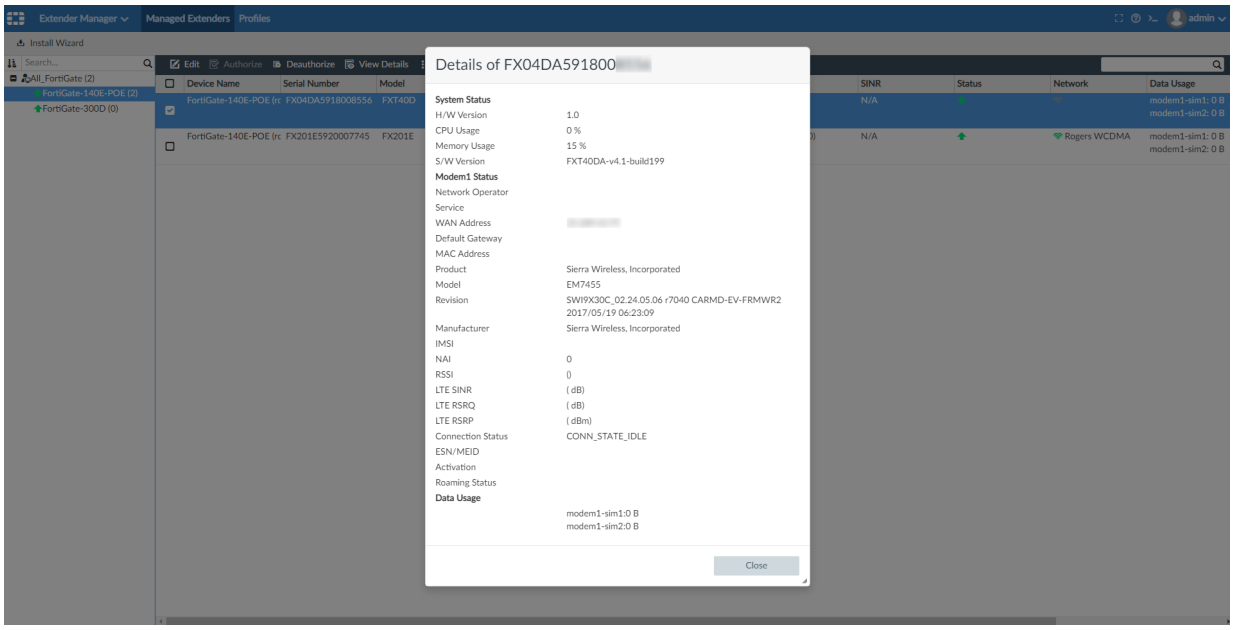
2. In the toolbar, double-click a device to edit it.



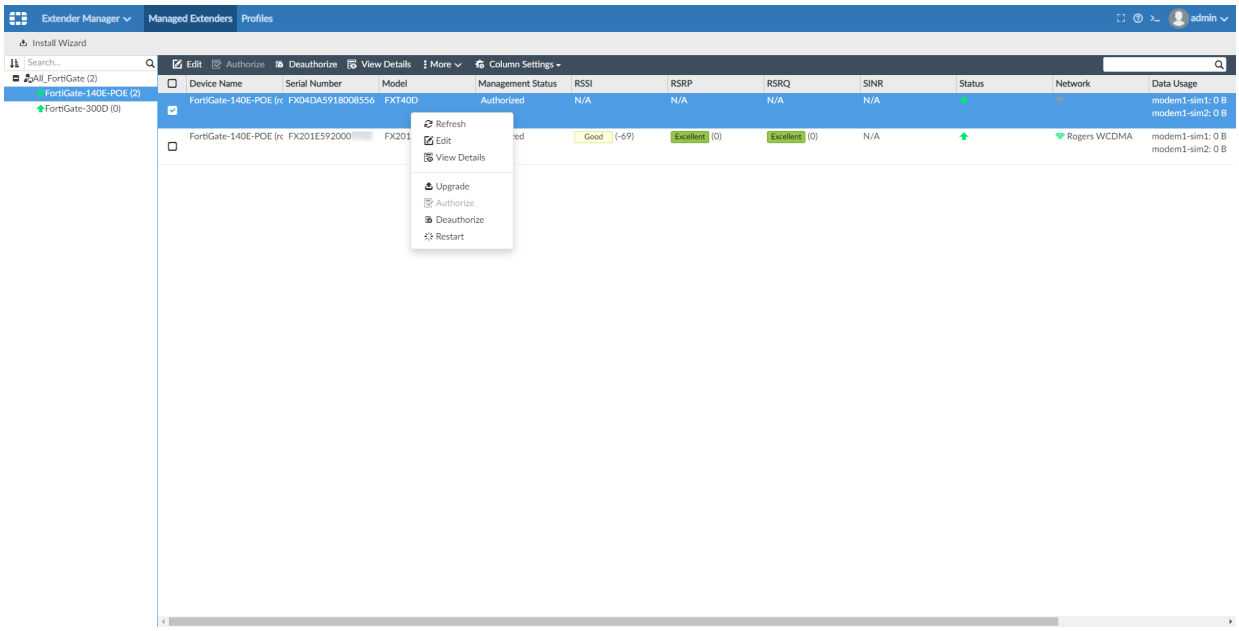
3. In the banner, click *Install Wizard* to install the changes on the device.



4. Right-click a device and click *View Details* to view the device information.

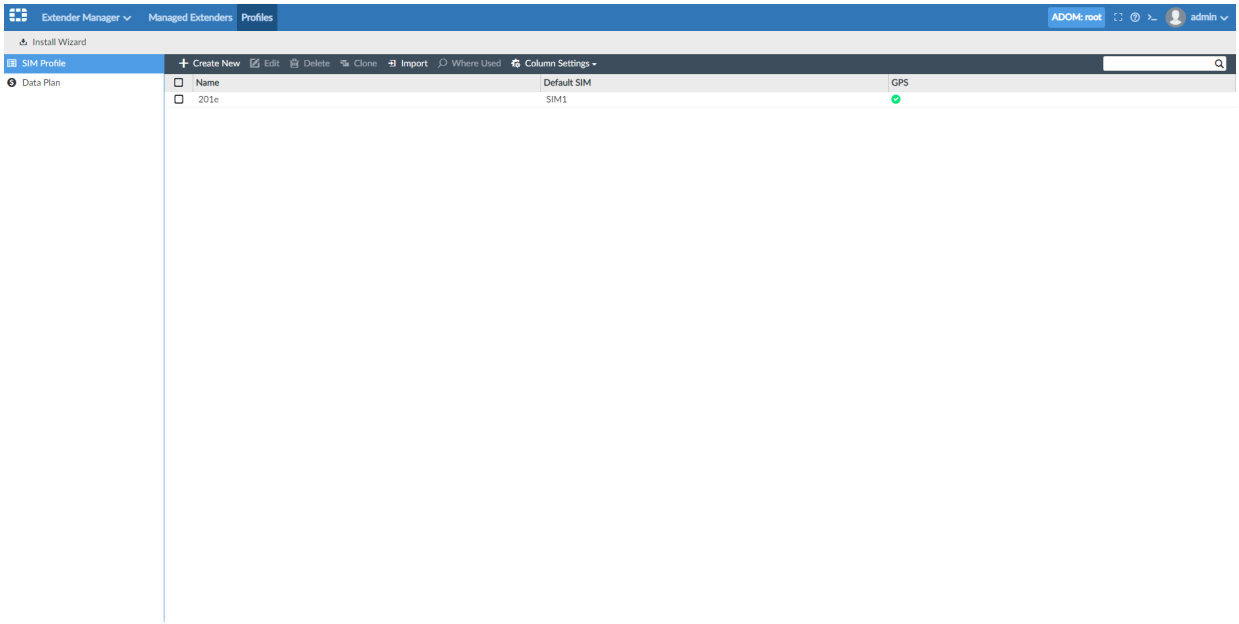


5. Right-click a device to *Upgrade*, *Deauthorize*, or *Restart* a device.



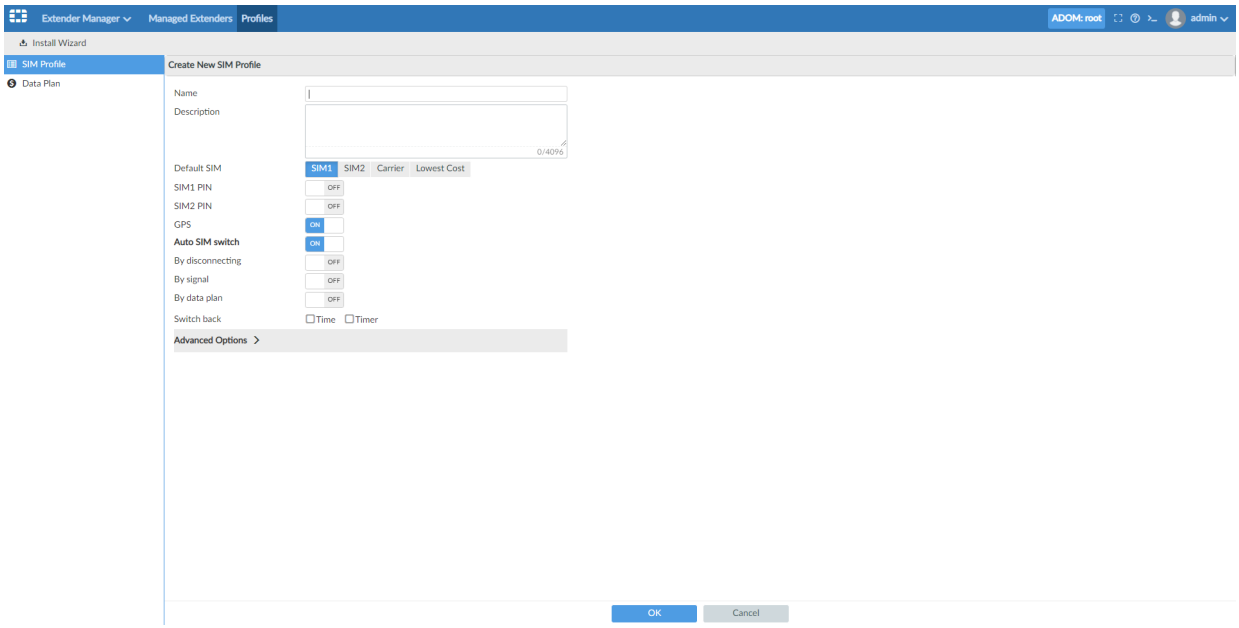
To manage a SIM profile:

1. Go to *Extender Manager* > *Profiles*.
2. In the tree menu click *SIM profile*.

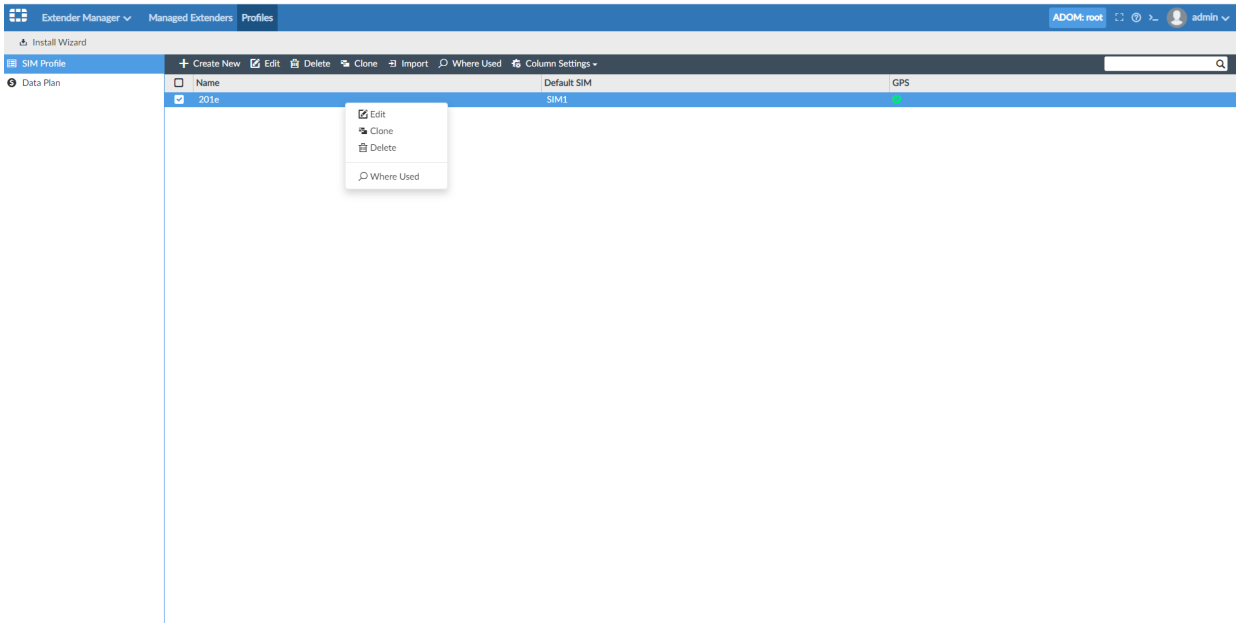


3. In the toolbar, click *Create New*.

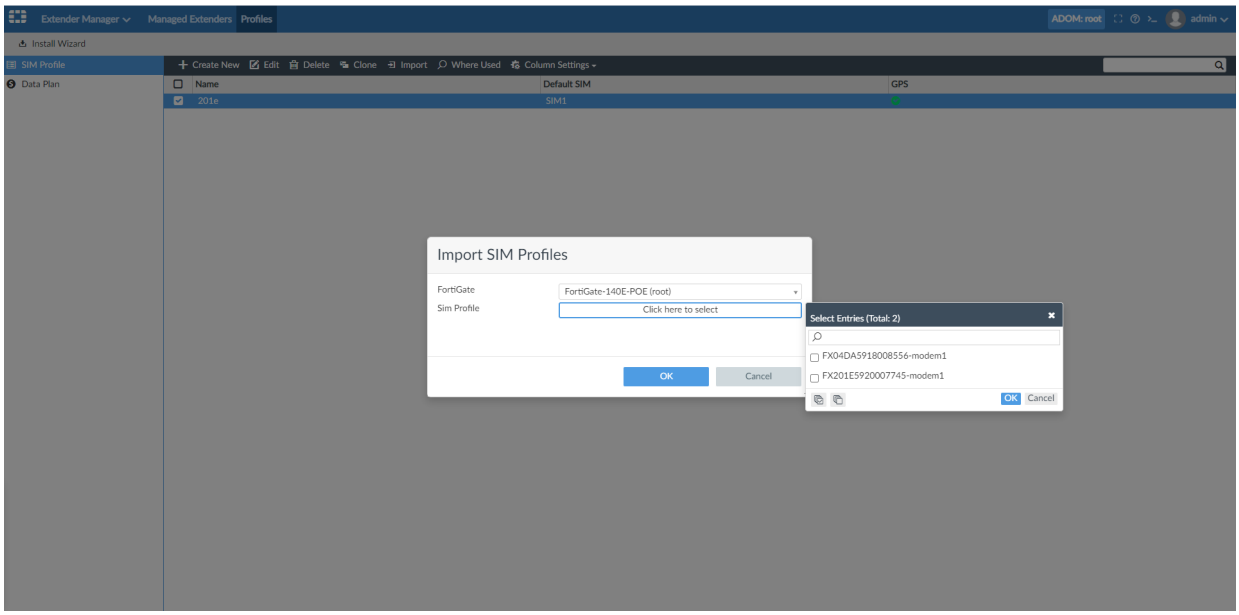
4. Configure the profile, and click *OK*.



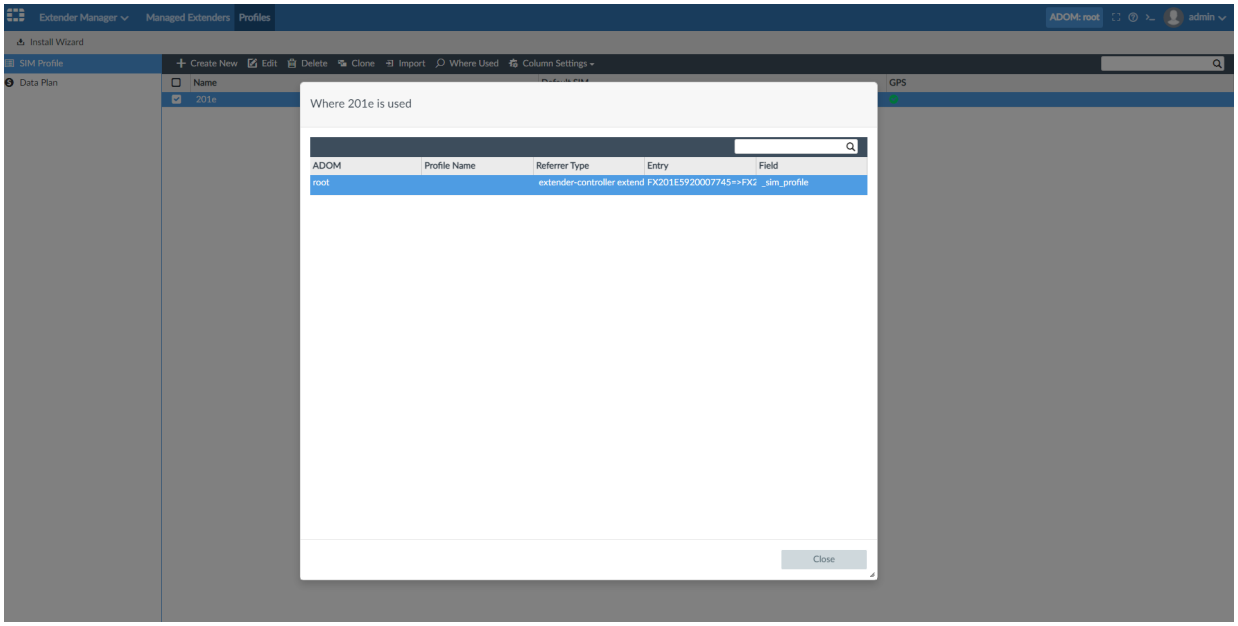
5. To clone a SIM profile, click *Clone* or right-click profile and select *Clone*.



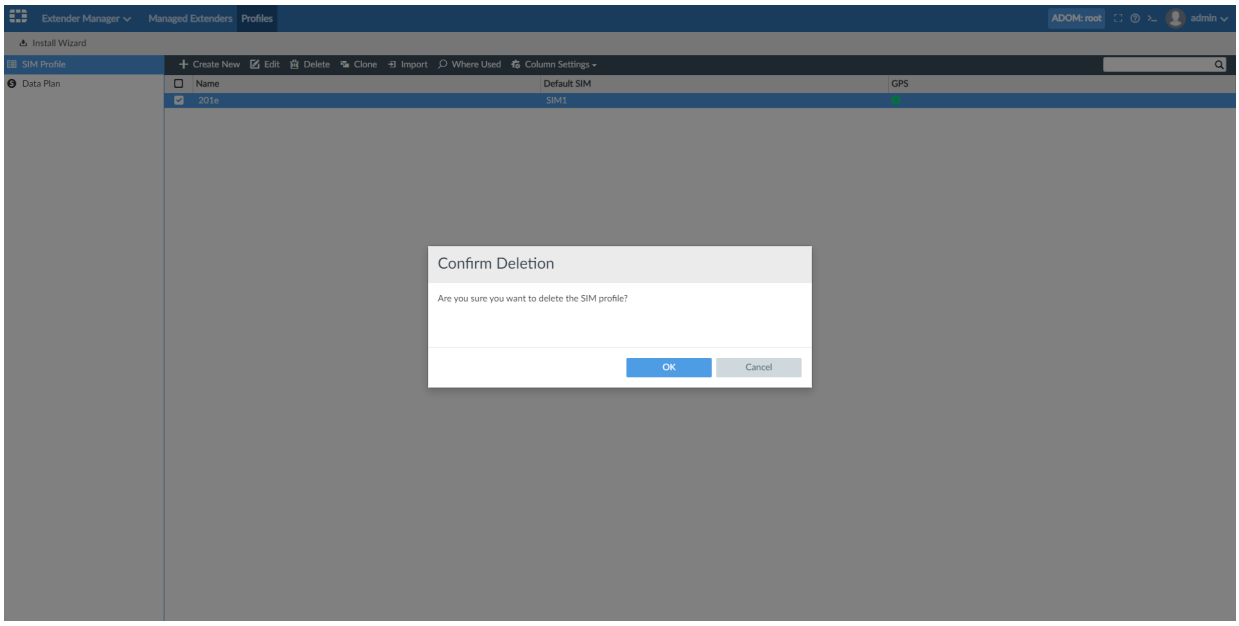
6. In the toolbar, click *Import* to import a profile from another device.



7. Click *Where used* to view where the profile is used.

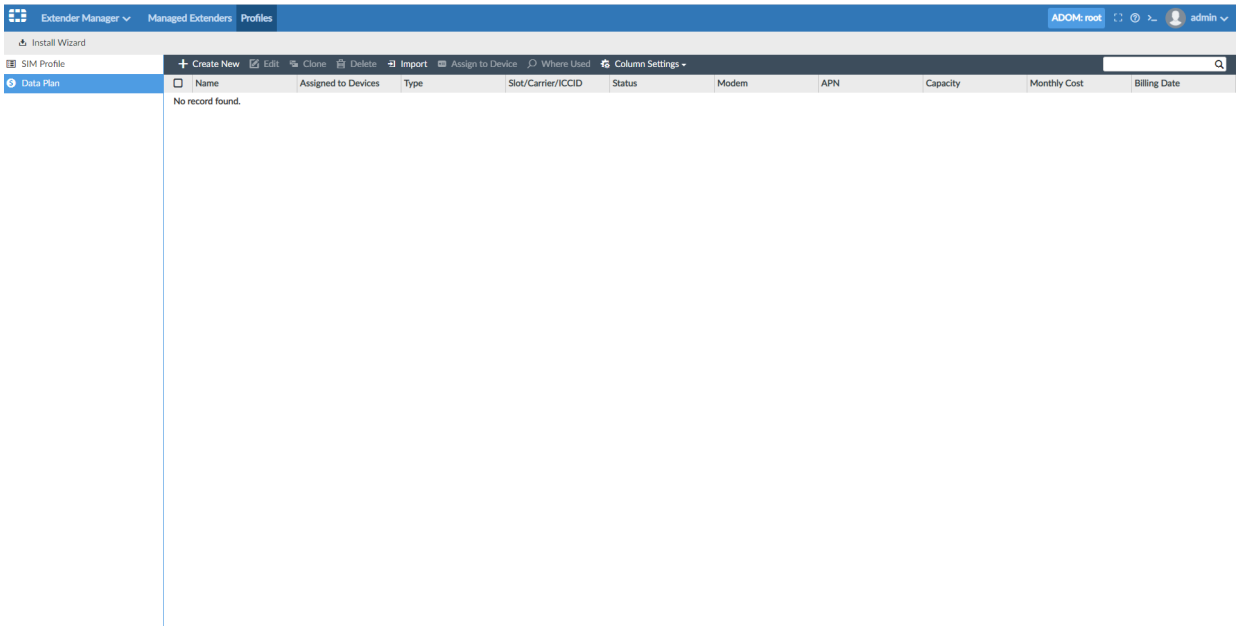


8. Click *Delete* to remove a profile. A profile that is in use cannot be deleted.

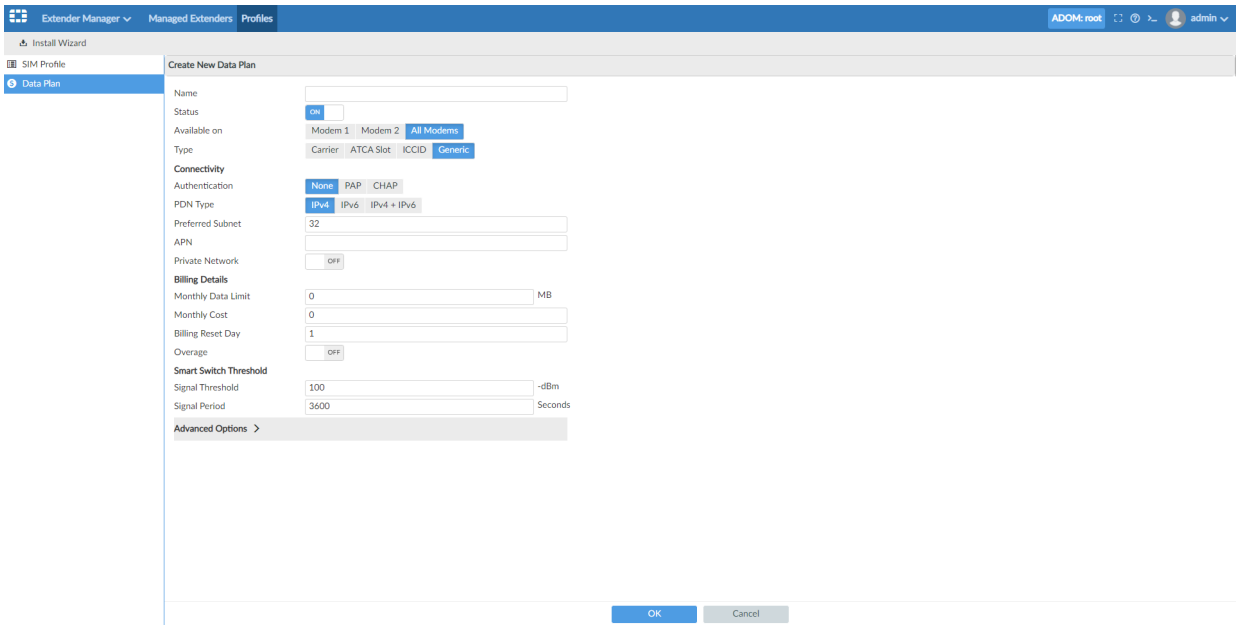


To manage a data plan:

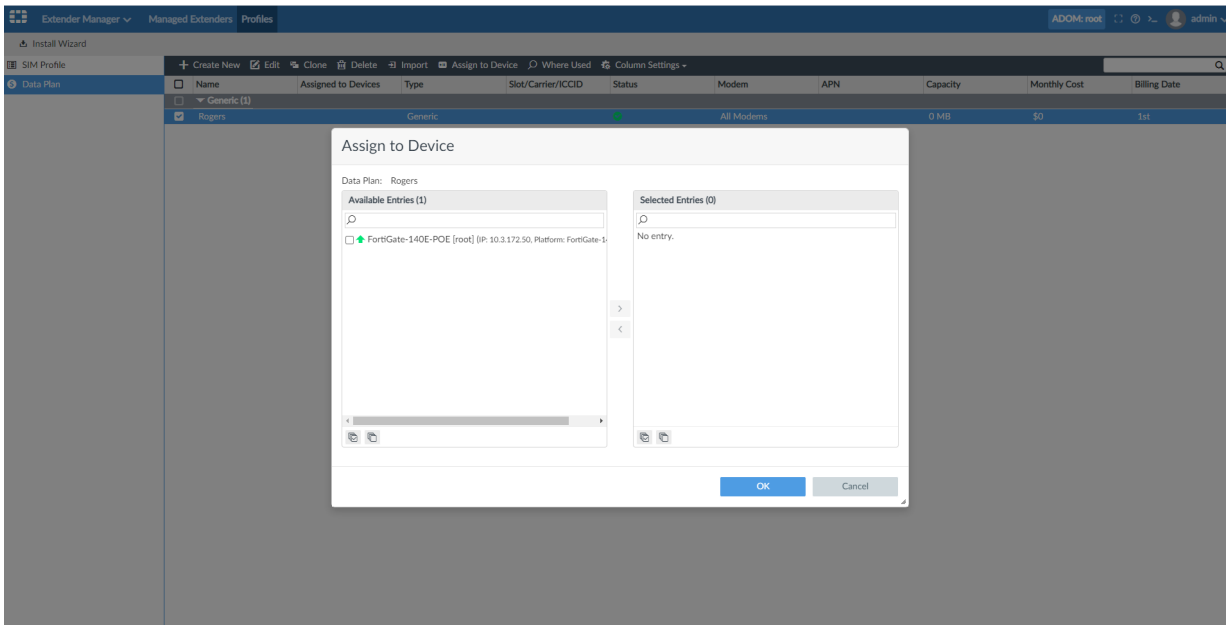
1. Go to *Extender Manager* > *Profiles*.
2. In the tree menu, click *Data Plan*.



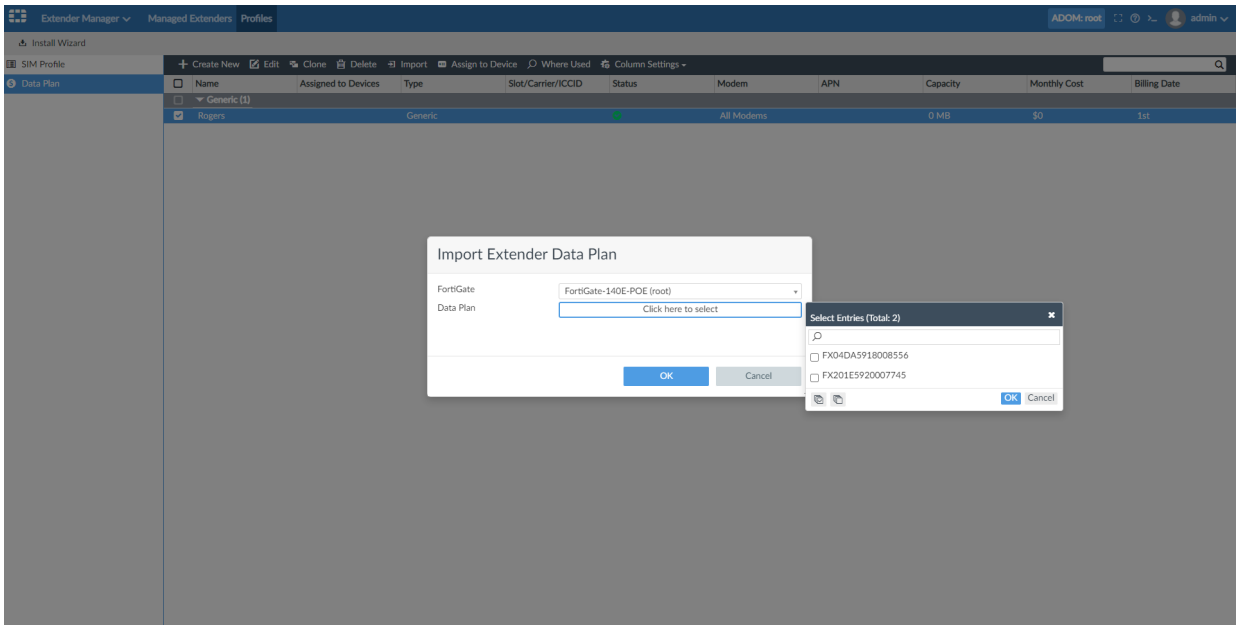
3. In the toolbar, click *Create New*. Configure the data plan settings and click *OK*.



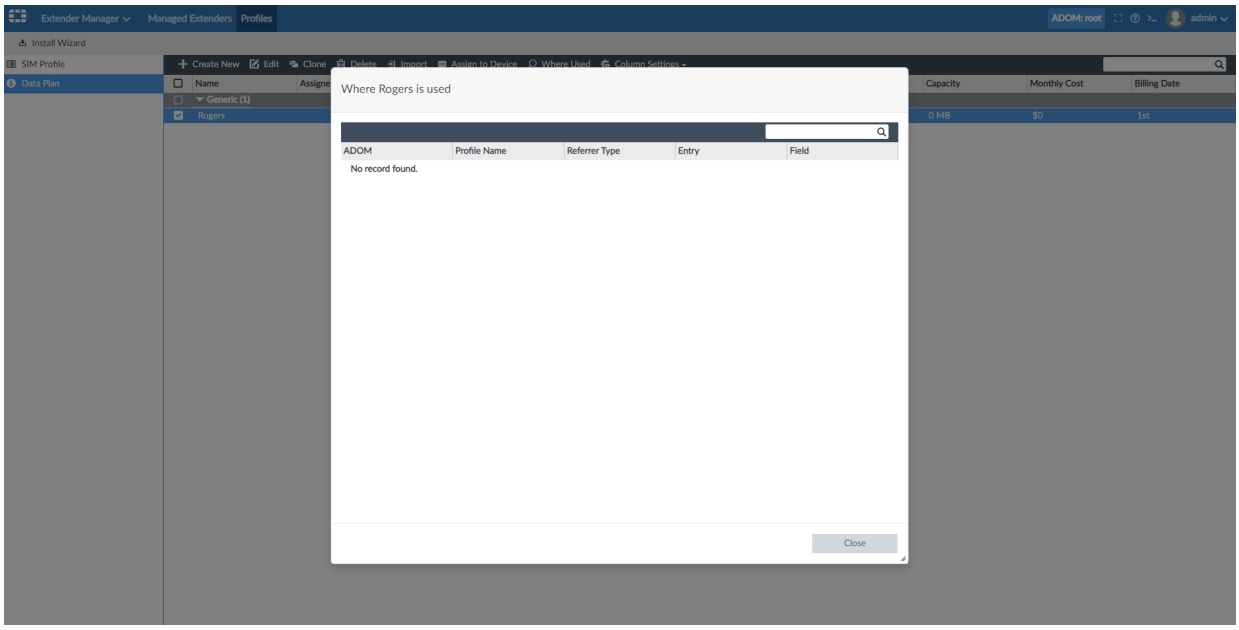
4. In the toolbar, click *Assign to Device* to install the plan on a device.



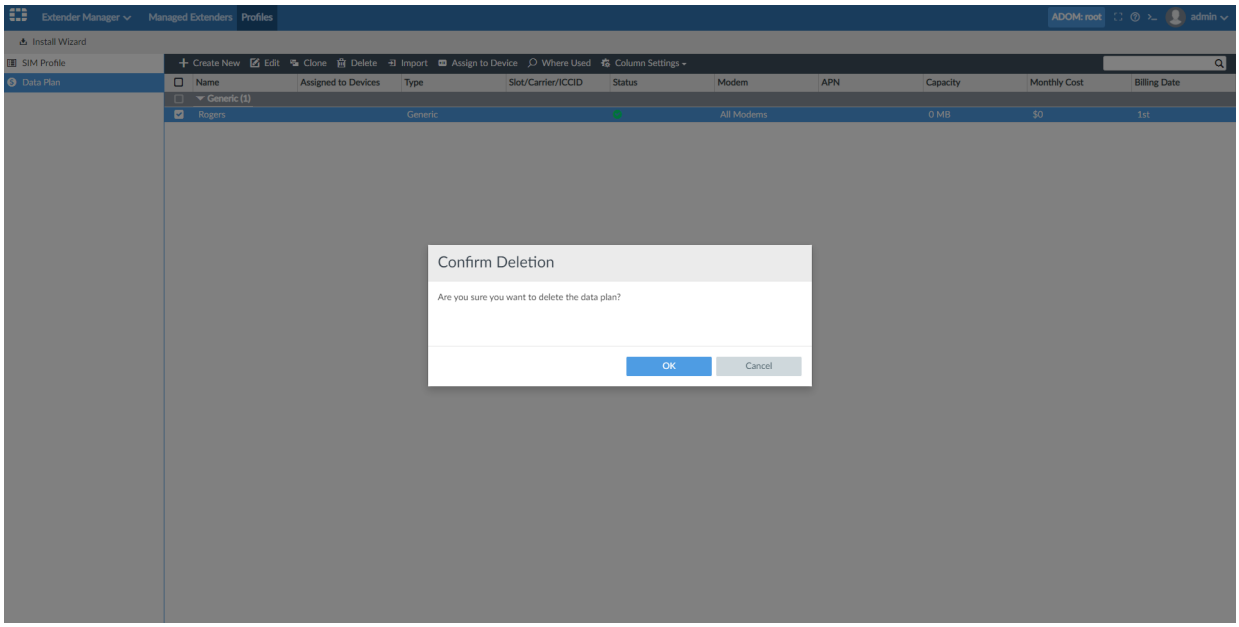
5. Click *Import* to import a data plan from the FortiGate settings. The data plan will be assigned to the FortiExtender where it is imported.



6. In the toolbar, click *Where Used* to view where the data plan is being used.



7. In the toolbar, click *Delete* to remove a data plan. You cannot delete a data plan that is in use.



Other

This section lists other new features added to FortiManager.

List of new features:

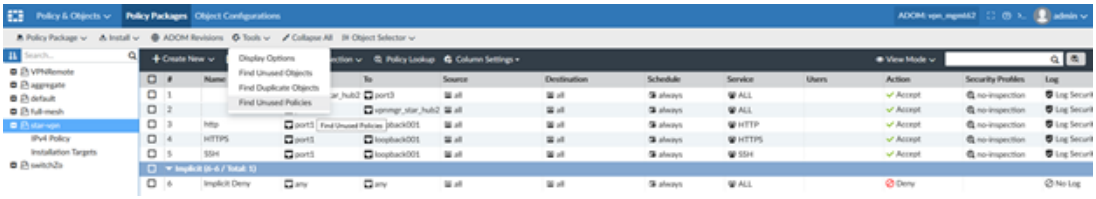
Policy Hit Count on unused policy - 6.4.3

When you run a policy check on a policy package or select the new *Find Unused Policies* option from the *Tools* dropdown for a policy package, FortiManager shows hit count information for unused policies with zero hit count.

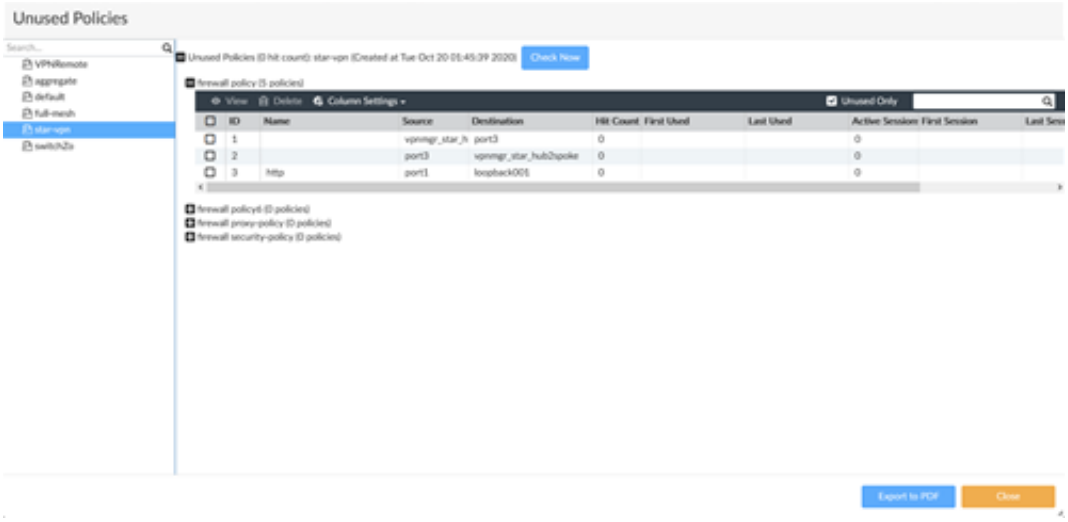
The *Find Unused Policies* option is unavailable when classic dual pane is enabled. To disable classic dual pane, go to *System Settings* > *Advanced* > *Advanced Settings*, and set the *Display Policy & Object in Classic Dual Pane* option to *Disable*.

To view the hit count information for unused policies using the new *Find Unused Policies* option:

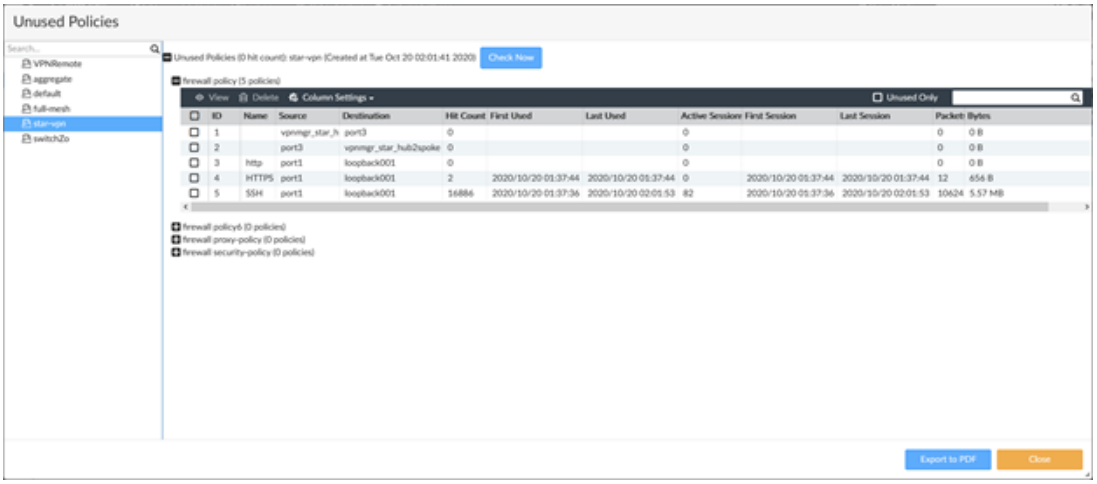
1. Go to *Policy & Objects* > *Policy Packages*.
2. In the toolbar, from the *Tools* dropdown, select *Find Unused Policies*.



   The *Unused Policies* window opens.
3. In the tree menu, select the policy package and expand the policy table of your choice in the content pane to see the hit count information.
   For instance, in the figure below, the star-vpn policy package is selected, and the firewall policy table with five policies is expanded.
   There are three unused policies with zero hit counts.

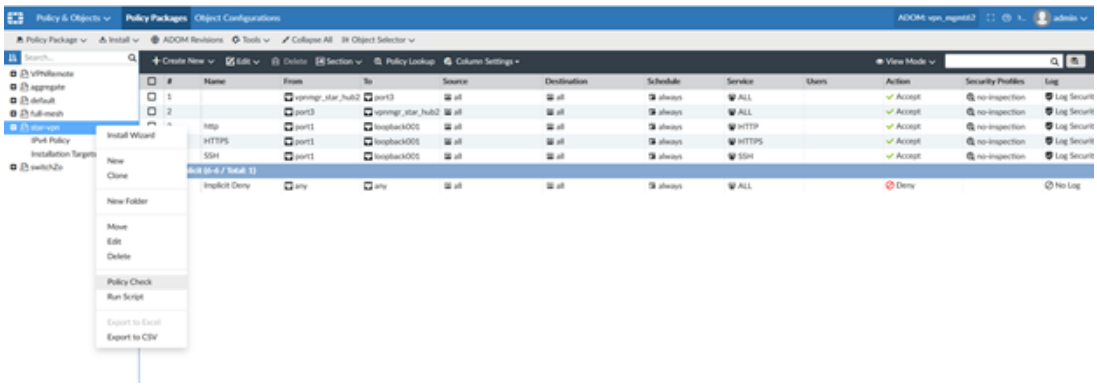


4. Clear the *Unused Only* checkbox to view all the policies.
   For example, the figure below displays the hit count information for all the policies including in use policies with ID 4 and 5.

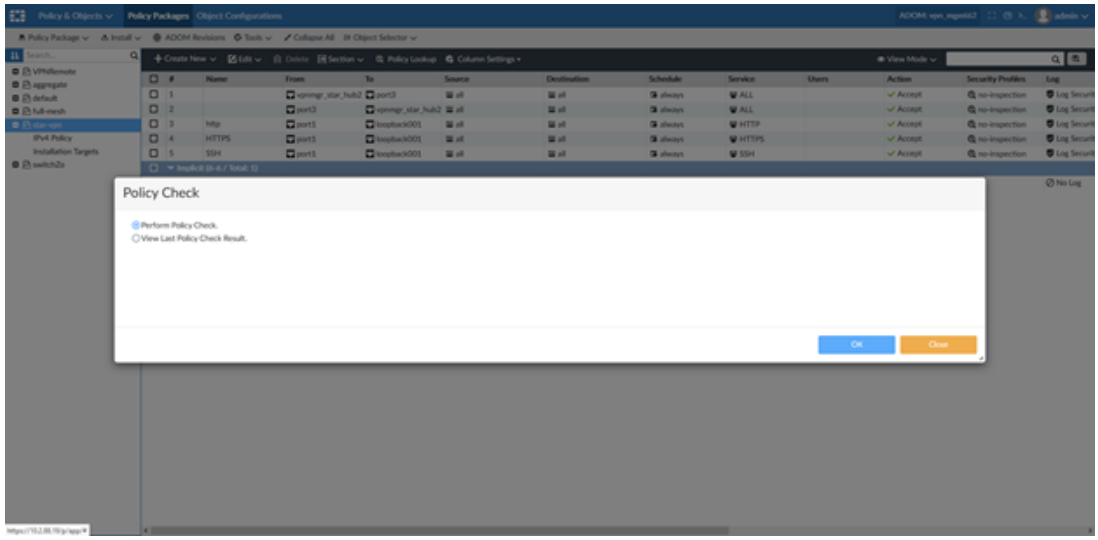


To view hit count information for unused policies in the Policy Check Report:

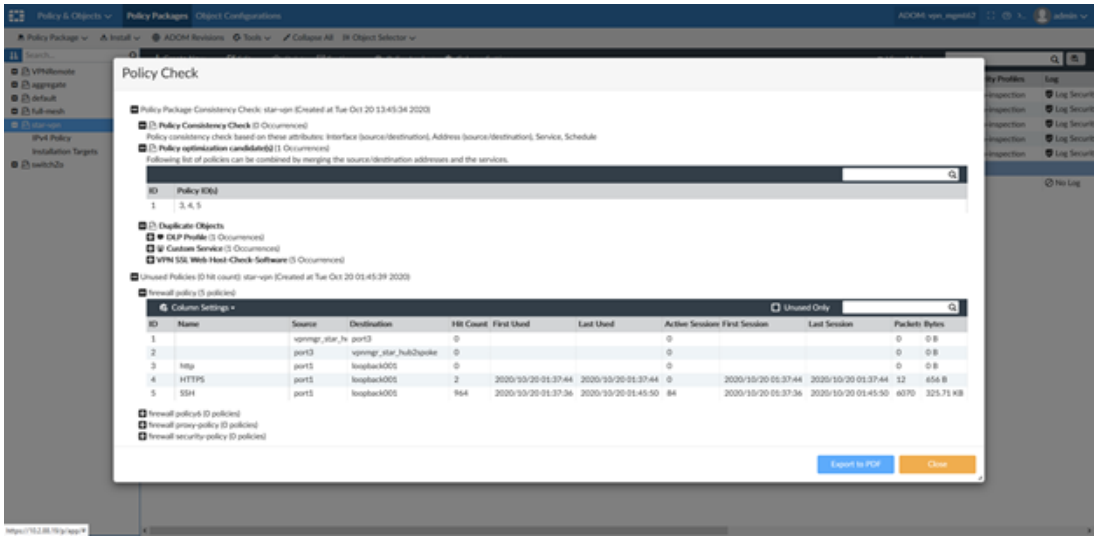
1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, right-click the policy package and select *Policy Check*.
   The *Policy Check* dialog opens.
   For example, in the figure below, the star-vpn policy package is selected for a policy check.



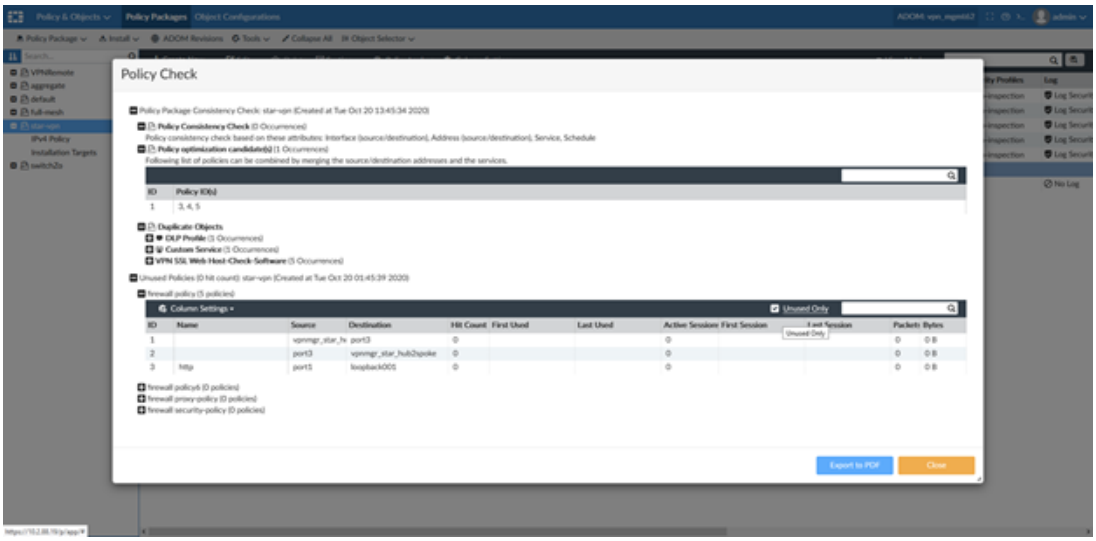
3. In the *Policy Check* dialog, click *Perform Policy Check*, and then click *OK*.



Once the policy check finishes, the results are displayed in the *Policy Check* window.
The *Policy Check* window displays the hit count information for all the policies in a policy package.



4. Select the *Unused Only* checkbox to view the hit count information for the unused policies only.



Normalized interface to map as zone only - 6.4.7

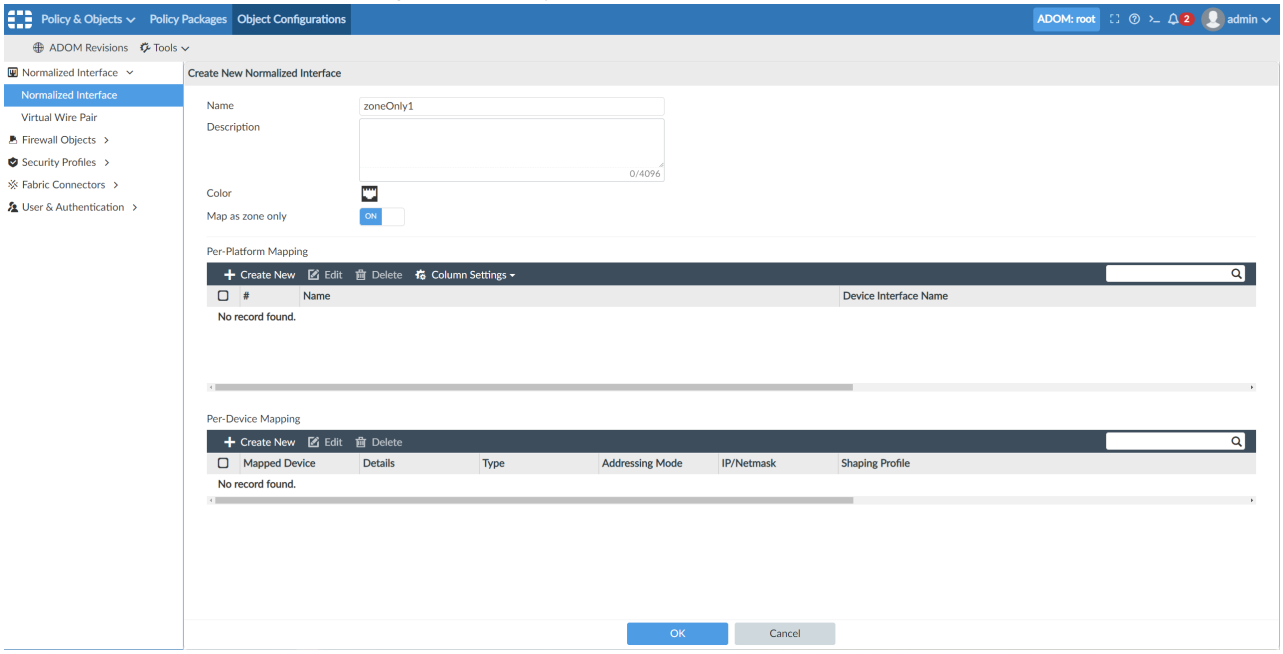
Starting in FortiManager 6.4.7, map as zone only mode is available for normalized interfaces.

To configure and use a normalized interface as zone only:

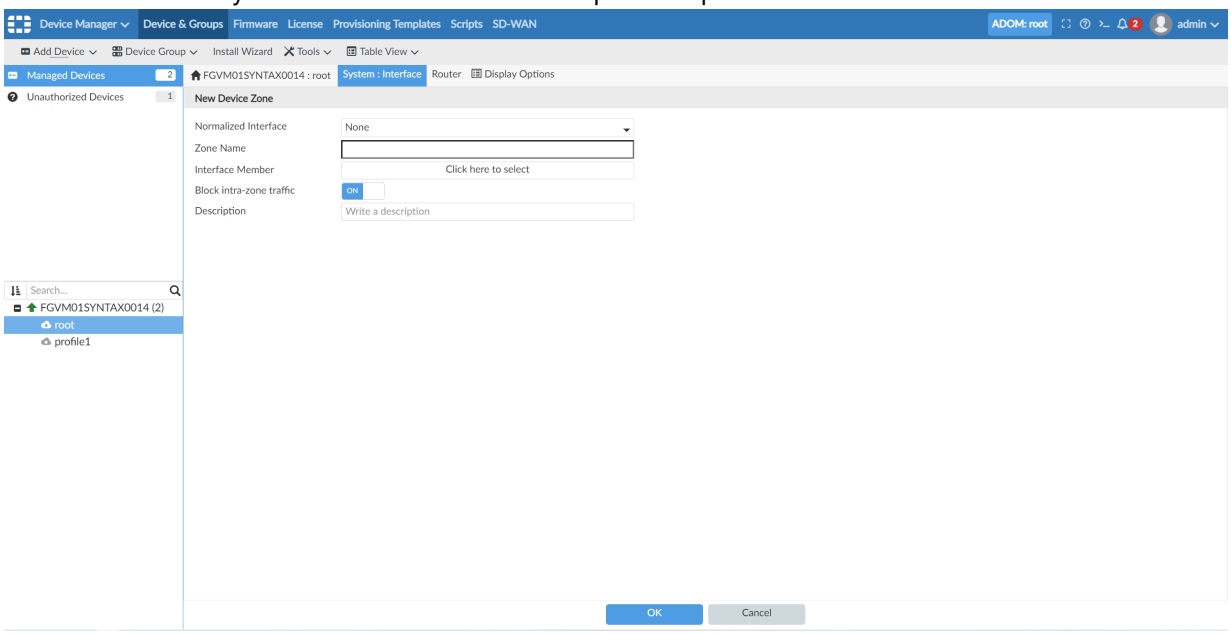
1. Enable mapping as zone only through the CLI with the following commands:

```
config system global
   set normalized-intf-zone-only enable
```

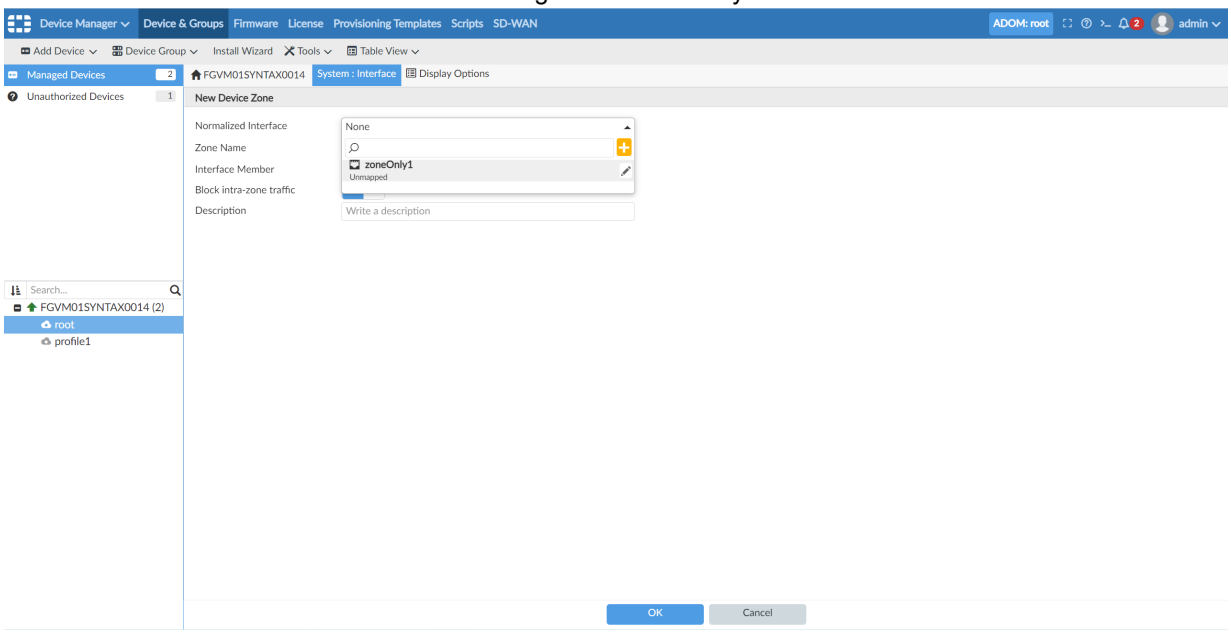
2. On FortiManager, go to *Policy & Objects* > *Object Configuration* > *Normalized Interface*, edit or create a new normalized interface, and select *Map as zone only*. Save the normalized interface.



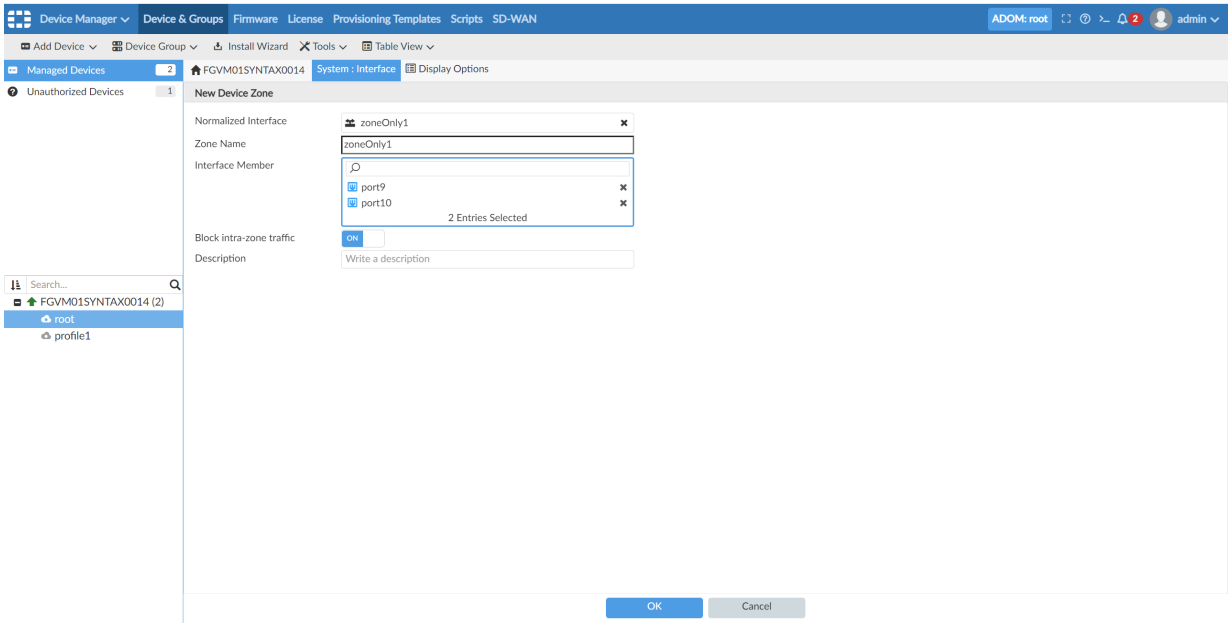
3. Go to *Device Manager* > *Device & Groups*, and create a new device zone.
   a. Normalized zone only name selection as well as the option to input a name are both available.



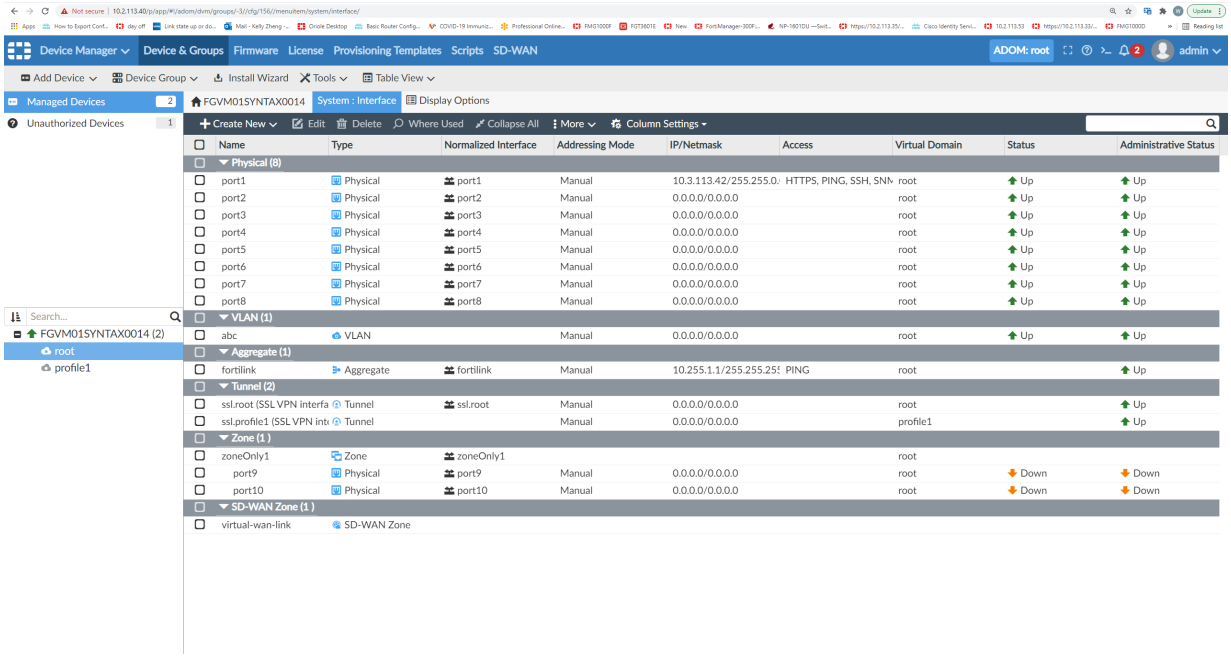
   b. Dynamic mapping is available in the table to filter by device zone and let the user select options only showing ADOM normalized interface zones that are configured as zone only.



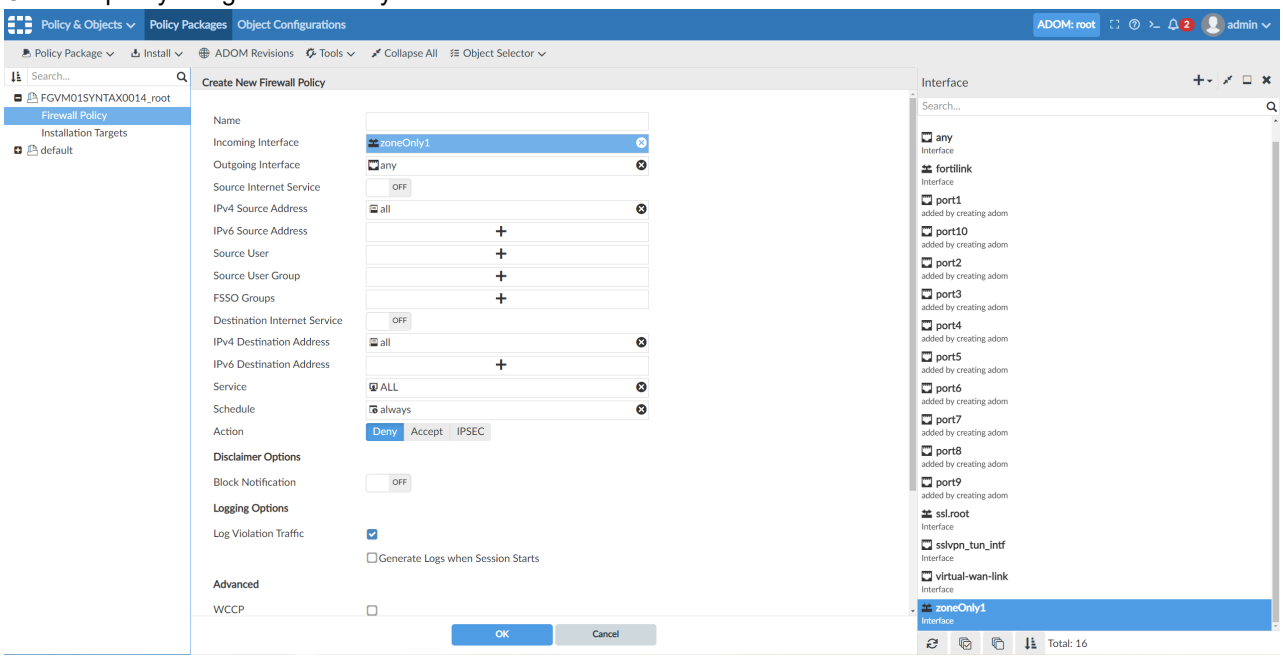
c. Once a zone is selected in the Normalized Interface field, if the zone name field is empty, the GUI will automatically fill the zone name input box.



d. After saving, the device zone is created.



4. Create a policy using the zone-only normalized interface.



5. Install and review the changes in the *Install Preview*.

```
config system zone
   edit "zoneOnly1"
      set interface "port9" "port10"
      next
   end
config firewall policy
   edit 3
      set uuid 34808cec-020f-51ec-64a0-f0c7e494e816
      set srcintf "zoneOnly1"
      set dstintf "any"
      set srcaddr "all"
      set dstaddr "all"
      set schedule "always"
      set service "ALL"
      set logtraffic all
      next
   end
```

6. After installation, FortiGate gets the configuration correctly.